

WatchGuard Command Line Interface Reference

Fireware XTM v11.3.5



Notice to Users

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.
Guide revision: February 21, 2012

Copyright, Trademark, and Patent Information

Copyright © 1998 - 2012 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.
Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at <http://www.watchguard.com/help/documentation/>.

ADDRESS

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

SUPPORT

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.613.0456

SALES

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895

ABOUT WATCHGUARD

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.
For more information, please call 206.613.6600 or visit www.watchguard.com.

Contents

Introduction to the CLI	1
About the CLI Reference Guide.....	1
Command reference format	1
Command reference notation.....	2
Sample command references.....	2
Start the Command Line Interface	3
Connect with serial cable.....	3
Connect with TCP/IP	4
Enter Commands in the CLI.....	5
Terminal commands	5
Get Help.....	5
help	5
Syntax used for help command.....	6
"?" command.....	8
Error Handling in the CLI	8
Import and Export Files	9
Command Modes Overview	11
Introduction to the CLI Command Modes.....	11
Main command mode.....	12
Configuration command mode.....	12
Interface command mode.....	12
Policy command mode.....	12
Common commands.....	13
Command Line Interface Prompt.....	13
Common Commands	15
List of Common Commands	15
Common Command Reference	16
exit.....	16
help	16
history	17
show	17
show cluster	18
show ip	18
show log-setting	18

show proposal.....	19
show objects.....	19
show bridge.....	19
show certificate.....	20
show ddns.....	20
show interface.....	20
show log-cache.....	20
show usb.....	21
show wireless.....	21

Main Command Mode 23

Enter the Main Command Mode.....	24
List of Main Mode Commands.....	24
Main Command Mode Reference.....	25
arp flush.....	25
backup image.....	25
cert-request.....	25
checksum.....	26
clock.....	26
configure.....	26
debug-cli.....	26
diagnose.....	27
diagnose to.....	27
diagnose cluster.....	27
diagnose hardware.....	27
diagnose vpn.....	28
dnslookup.....	31
export.....	31
import.....	32
password.....	32
ping.....	32
reboot.....	32
restore.....	33
shutdown.....	33
sync.....	33
sysinfo.....	34
tcpdump.....	34
traceroute.....	34
upgrade.....	34
usb.....	35
vpn-tunnel.....	35
who.....	35

Configuration Command Mode 37

Enter the Configuration Command Mode.....	38
List of Configuration Mode Commands.....	38
Configuration Command Mode Reference.....	39
auth-setting.....	39
bridge.....	40
cluster.....	40
ddns.....	42
default-packet-handling.....	42

global-setting	43
interface	44
ip	45
log-setting	47
managed-client	48
modem	49
multi-wan.....	50
network-mode	52
ntp	53
policy	53
signature-update	54
snmp	54
static-arp	55
system	55
vlan.....	56
vpn-setting.....	56
web-server-cert	57
wireless	58

Interface Command Mode 63

Enter the Interface Command Mode	64
List of Interface Mode Commands	64
Interface Command Mode Reference	65
dhcp.....	65
enable	66
ip	66
link-speed	66
mac-access-control	67
mac-ip-binding.....	67
mtu.....	67
name.....	68
pppoe.....	68
qos.....	69
secondary	70
type	70
vpn-pmtu.....	70

Policy Command Mode 71

Enter the Policy Command Mode	72
List of Policy Mode Commands	72
Policy Command Mode Reference	73
alias	73
apply.....	74
auth-server	75
auth-user-group.....	76
bovpn-gateway	77
bovpn-tunnel	79
dynamic-nat.....	81
mvpn-ipsec.....	82
mvpn-rule	85
one-to-one-nat.....	87
policy-type	87

pptp	88
proposal	88
rule	89
schedule	93
sslvpn	93
traffic-management.....	95
user-group.....	95
users.....	95

Index	97
--------------------	-----------

1 Introduction to the CLI

WatchGuard® Firebox® X e-Series and WatchGuard XTM devices with Fireware XTM v11.x OS include a Command Line Interface (CLI) installed on the hardware. You can connect to the device and use the CLI as an alternative to the Web UI or WatchGuard System Manager software. You can use the CLI with any terminal client that supports SSH2.

About the CLI Reference Guide

This section provides information about how to use the command reference in this document.

Command reference format

The syntax section for each command uses a table format:

This line shows a single syntax for a command and uses the notation described in the subsequent section.
--

This line contains the guidance and comments for the command. For commands where a choice is available for a particular portion of the command, all possible options are described. In the case where a command requires no guidance or comments, this line contains the text "No options available."

Command reference notation

The syntax section of each command uses a standardized format and notation:

Notation	Required	Optional	Meaning	Example
text	✓		Must be typed exactly as shown.	show
text	✓		The requested information is required. Examples include an account name, password, or IP address.	accountname
<i>string</i>	✓		When information must be selected from a series of options, these appear in the command guidance.	<i>blocked-site</i> or <i>allowed-site</i>
<u>text</u>		✓	An additional parameter that, when used, changes the behavior of the command.	<u>log</u>
<i>text</i>		✓	Additional information that, when provided changes the behavior of the command.	<i>text</i>
text <i>string</i>		✓	An extension or option to expand the functionality of the original command. Both text and <i>string</i> are required to complete the additional parameter. text must be entered as is, and <i>string</i> is required information.	count in

Sample command references

A command reference provides:

- The command
- A brief description of the command
- The command syntax
- Examples, where appropriate

The subsequent commands are two sample command references. Where appropriate, the example also includes sample output.

history

Description: Display the command history list with line numbers.

Syntax:

history
No options available.

export

Description: Export information to an external platform or file.

Syntax:

export <i>type</i> to <i>location</i>
Export the blocked sites or allowed sites list to a file. <i>type</i> must be one of these options: <i>blocked site</i> or <i>allowed-site</i> <i>location</i> must be either an FTP or TFTP address.
export <i>config</i> to <i>location</i>
Export the XTM device configuration to a file. <i>location</i> must be either an FTP, TFTP address or console.
export <i>muvpn</i> <i>muvpnid</i> <i>client-type</i> <i>client</i> to <i>location</i>
Export the Mobile VPN with IPSec client configuration to a file. <i>muvpnid</i> must be an existing Mobile VPN with IPSec group. <i>client</i> must be one of these options: <i>watchguard</i> or <i>shrew-soft-client</i> . - <i>watchguard</i> — export the .ini profile for use with the WatchGuard Mobile VPN with IPSec client. - <i>shrew-soft-client</i> — export the .vpn profile for use with the Shrew Soft VPN client. <i>location</i> must be either an FTP, TFTP address or console.
export <i>support</i> to <i>location</i>
Export support information to a file. <i>location</i> must be either an FTP or TFTP address.

Example:

```
export blocked-site to ftp://joez:1pass@ftp.bigco.com:23/upload/blocked.dot
export muvpn ipsec-users client-type shrew-soft-client to ftp://
joez:1pass@ftp.bigco.com:23/upload/ipsec-users.vpn
```

Start the Command Line Interface

To connect to the WatchGuard® CLI, you use a terminal client located in the same secure environment as the WatchGuard device. The terminal client must use SSH2 to connect to the WatchGuard device with a serial cable. You can also connect to the Console port or with TCP/IP to a Trusted or Optional interface. You can use the CLI to manage the WatchGuard device while it is in operation, though some configuration changes require a restart.

Connect with serial cable

To manage a WatchGuard device with a serial cable connection, your computer must have an available serial port and an installed terminal client application.

- 1 Connect a serial cable from your computer to the Console port on the WatchGuard device.
- 2 Open your terminal application. Open a new connection window.

- 3 Verify that the terminal is set to VT100. Verify that your connection parameters are set to:

Setting	Value
Port	The serial port on your management computer, usually COM1
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	No
Flow Control	None



If the terminal is not set to VT100, some command and control key functions do not work. For example, Ctrl-C does not break, some special characters do not type, and ESC does not work.

- 4 Press <ENTER>.
The connection window displays a welcome message and the WatchGuard device login prompt.
- 5 Type the administrator user name. Press <ENTER>.
There are two default administrator accounts: admin and status. Use admin for read-write privileges. Use status for read-only privileges.
- 6 Type the administrator read-write password. Press <ENTER>.
The default password for the admin account is readwrite. The default password for the status account is readonly. The WatchGuard CLI opens in the Main command mode with the prompt WG#.

Connect with TCP/IP

The default WatchGuard policy allows you to connect to and manage a WatchGuard device from any computer on a trusted or optional network on port 4118. For more information about how to modify the default policy to either restrict access to the CLI or enable access from an external network, see the *Fireware XTM WatchGuard System Manager Help*.

For this procedure, you must have a terminal client that supports SSH2 and the IP address of a WatchGuard device trusted or optional interface.

- 1 Open your terminal application. Open a new connection window.
- 2 Verify that the terminal is set to VT100. Verify that your connection parameters are set to:

Setting	Value
Host	The IP address of the Firebox or XTM device trusted or optional interface
TCP Port	4118
Service	SSH (version SSH2)
Protocol	IPv4



If the terminal is not set to VT100, some command and control key functions do not work. For example, Ctrl-C does not break, some special characters do not type, and ESC does not work.

- 3 Press <ENTER>.
The connection window displays a welcome message and the WatchGuard device login prompt.
- 4 Type the administrator user name and password.
There are two default administrator accounts: admin and status. Use admin for read-write privileges. Use status for read-only privileges. The default password for the admin account is readwrite. The WatchGuard CLI opens in the Main command mode with the prompt WG#. The default password for the status account is readonly. The WatchGuard CLI opens in the Main command mode with the prompt WG>.

Enter Commands in the CLI

To use the WatchGuard CLI, type a command at the prompt and press Enter on your keyboard. It is not necessary to type the command in full to have the CLI execute the command correctly.

Terminal commands

The subsequent table includes a series of commands to move around in, and to operate in, the CLI.



Your terminal client can use different commands or operating system rules for the procedures in this section.

Keyboard Key(s)	Function
Backspace	Erase the character to the left of the cursor. If there is no character to the left of the cursor, erase the current character.
Ctrl D	Erase the current character at the cursor.
Ctrl K	Erase all characters from the cursor to the end of the current command line.
Esc D	Erase from the cursor to the end of the current word.
Ctrl W	Erase from the word to the left of the cursor.
Ctrl B or Ctrl ←	Move the cursor to the left one character.
Ctrl F or Ctrl →	Move the cursor to the right one character.
Ctrl A	Move the cursor to the start of the line.
Ctrl E	Move the cursor to the end of the line.
Esc B	Move the cursor to the left one word.
Esc F	Move the cursor to the right one word.
Ctrl P or Ctrl ↑	Recall commands in the history buffer.
Ctrl N or Ctrl ↓	Recall recent commands.
Ctrl T	Replace the character to the left of the cursor with the character at the cursor.
Ctrl L	Show the current command line again.

Get Help

The WatchGuard® Command Line Interface (CLI) has an interactive Help system. To use the Help system, type **help** or **?** at the command line and press Enter.

help

Description: Display a numbered list of the available command formats for the specific command.

Syntax:

help command
If no command provided, describes general features of the Help system.
If command provided, returns a list of all the possible syntaxes for the specified command.
If ? provided for command, returns a list of all commands for which help is available in current command mode.
command must be a valid command for the current command mode.

Example:

```

help arp
  [1] arp (flush)

help diagnose
  [1] diagnose [to(<ftp>|<tftp>)|cluster[to(<ftp>|<tftp>)]]
  [2] diagnose vpn<ident>

help export
  [1] export (blocked-site|allowed-site) to (<ftp>|<tftp>)
  [2] export (config) to (<ftp>|<tftp>|console)
  [3] export muvpn <ident> to (<ftp>|<tftp>|console)
  [4] export support to (<ftp>|<tftp>)

help ping
  [1] ping <mstring>

help tcpdump
  [1] tcpdump [<mstring>]*

```

Syntax used for help command

The help command uses a unique syntax to describe how to use CLI commands.

Element	Example	Usage
	<ftp> <tftp>	Indicates that the command allows any one of the options separated by the .
[]	[to (<ftp> <tftp>)]	Indicates that the text provided between the [and] can optionally be used in the command.
*	[<ident>]*	Indicates that multiple items can be added to the command.
()	(blocked-site allowed-site)	Indicates the text between the (and) is required.
< >	<alarm event traffic debug>	Indicates that information or a selection identified by the text between the ≤ and ≥, must be made by the user.
<ident>	(batch secret <ident> secret)	Indicates that a specific piece of information is required to execute this command. This information could be an account name, a password, or the name of a certificate. Use the ? command to determine what the required information is, or refer to the command reference provided in this document. Must be enclosed by double quotes.
<ftp>	[to (<ftp> <tftp>)]	Indicates that an FTP address in the required format is accepted by the command. See "Import and Export Files" on page 9 for the required format.
<tftp>	[to (<ftp> <tftp>)]	Indicates that a TFTP address in the required format is accepted by the command. See the subsequent section for the required format.

Element	Example	Usage
int:x-y	<int:0-int_max>	Indicates that an integer between the specified range of X and Y must be provided. If Y is 'int_max' the maximum value allowed is 2147483647.
<ipaddr>	(<ipaddr> <ipmask> <net>)	Indicates a Version 4 IP address (IPv4), or a dotted decimal notation in the form of nnn.nnn.nnn.nnn where nnn is 0–255 is required. Used with <ipmask>.
<ipmask>	(<ipaddr> <ipmask> <net>)	Indicates a Netmask in the form of mmm.mmm.mmm.mmm where mmm is 0–255 is required. Used with <ipaddr>.
<net>	(<ipaddr> <ipmask> <net>)	Indicates a Classless InterDomain Routing (CIDR) notation is required in the form of nnn.nnn.nnn.nnn/dd where nnn is 0–255 and dd is 0–32.
<macaddr>	<macaddr>	Indicates a physical address of a device is required. Format must be 01:23:45:67:89:ab.
<cr>	<cr>	Indicates that the command line is complete and can be executed when you press "Enter".
<mstring>	<p>ping <mstring></p> <p>where <mstring>: [-LRUbdfnqrVvAA] [-c count] [-i interval] [-w deadline][hop1...] [-p pattern] [-s packetsize] [-t ttl] [-I interface or address] [-M mtu discovery hint] [-S sndbuf] [-T timestamp option] [-Q tos] [-i interface] [-s snaplen] [-T type][expression]</p> <p>traceroute <mstring></p> <p>where <mstring>: [-adhrvAMOO] [-w wait] [-S start_ttl] [-m max_ttl] [-p port#] [-q nqueries] [-g gateway] [-t tos] [-s src_addr] [-g router] [-l proto] host [data size]</p> <p>tcpdump <mstring></p> <p>where <mstring>: [-adeflnNOPqStuvvX][-c count] [-i interface] [-s snaplen] [-T type][expression][</p>	Indicates multiple strings of optional and required attributes as an argument of a command.

“?” command

Description: Displays all possible options for the next part of a command.

Syntax:

command ?

command must be a valid command for the current command mode. If not a valid command, the CLI returns “Unrecognized command”.

To display a list of all available commands for the current command, leave ***command*** blank.

If the CLI returns <cr> Carriage return, it indicates that the command can be executed as entered.

Example:

```
show s?
  schedule          Schedule for use in the application of policies
signature-update   Signature update configuration
snmp               Simple Network Management Protocol
sslvpn            Secure Sockets Layer Virtual Private Network
static-arp         Static ARP entries
status-report      Display system status
sysinfo           Display system information
```

Error Handling in the CLI

When you type a command that returns an error, the WatchGuard CLI shows:

- Where the error is in the syntax,
- The part of a command that is not recognized, or
- Other feedback on the error message.

There are five error message categories in the CLI: unrecognized, incomplete, execution, syntax, and ambiguous.

Unrecognized Command Error

If a command does not exist, the CLI returns an unrecognized command error.

For example, in the Main command mode, the user enters the command **help acc**. Because there are no commands in the Main mode which start with “acc”, the CLI returns the message

```
% Unrecognized command.
```

Incomplete Command Error

If a user enters a command without all the required parameters, the CLI returns an incomplete command error.

For example, in the Main command mode the user enters the command **show**. Because the show command requires an additional parameter to indicate what should be displayed, the command is incomplete, and the CLI returns the message % Incomplete command.

Execution Error

If a user enters a command with incorrect information, the CLI returns an execution error.

For example, in the Main command mode, the user enters the command **show users user1000**.

Because there is no user1000, the command is inaccurate, and the CLI returns the message

```
% Error: Account 'user1000' not found.
```

The error message includes information to help the user identify the error and correct the command.

Syntax Error

If a user enters a command incorrectly, the CLI returns a syntax error. The error message is:
% Invalid input detected at '^' marker, where the ^ marker denotes the start of the invalid command.

Ambiguous Command Error

If a user enters a truncated command that has more than one possible meaning, the CLI returns an ambiguous command error. The error message is: % Ambiguous command input detected at '^' marker where the ^ marker denotes the start of the ambiguous input.

Import and Export Files

With the CLI, you can export and import files between a WatchGuard device and a remote server with either FTP or TFTP. The address must include a file name and the complete URL path, where appropriate.

The FTP address must use this syntax to identify the user, server, and filename:

```
ftp://[user[:passwd]@]host[:port]/[complete URL path]/filename
```

Example:

```
ftp://ftpuser:ftppassword@ourftpsite:23/files/upload/file.dot  
ftp://ftpuser:ftppassword@ourftpsite:23/readme.txt
```

The TFTP address must use this syntax to identify the server and file:

```
tftp://host/url-path
```

Example:

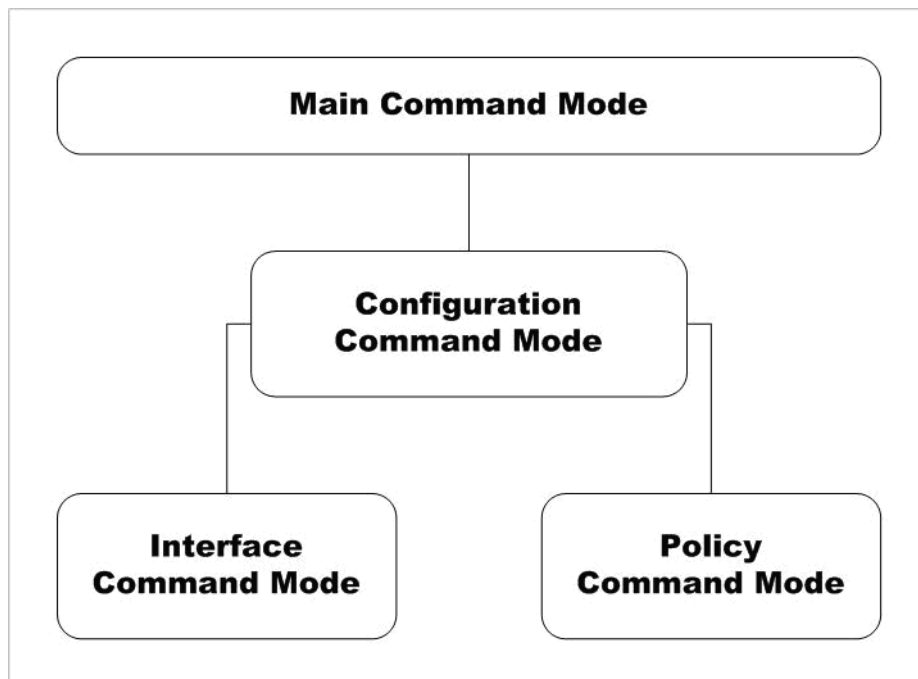
```
tftp://myftpsite/files/upload/file.dot
```


2 Command Modes Overview

The WatchGuard Command Line Interface (CLI) operates in four distinct command modes: Main, Configuration, Policy, and Interface. This section gives an overview of the command modes and how to use the command prompt to identify the working mode.

Introduction to the CLI Command Modes

The command mode hierarchy describes the relationship between the four command modes. To get access to the Configuration command mode, you must be in the Main command mode. To get access to the Interface and Policy command modes, you must be in the Configuration command mode.



Main command mode

The Main command mode is the default command mode of the WatchGuard CLI. In Main mode, you can:

- Modify some higher level configuration settings
- See system logs
- Enter the Configuration command mode
- Restore or upgrade the software image
- Shut down or reboot the WatchGuard device

Configuration command mode

The Configuration command mode is used for system and network configuration of the Firebox or XTM device. To get access to the Configuration command mode, open the CLI in the Main command mode, then use the command **configure**. You can use Configuration mode to perform these functions:

- Manage the logging performed by the Firebox or XTM device
- Configure global network settings
- Enter the Policy and Interface command modes

Interface command mode

The Interface command mode is used to configure the Ethernet interfaces of the WatchGuard device. To get access to Interface command mode, open the CLI in Configuration command mode, then use the command **interface**. You can use Interface command mode to perform these functions on a single interface:

- Configure the IP address and addressing options for the interface
- Configure the interface as a gateway
- Control MTU and link speed preferences
- Configure the interface as a DHCP server or DHCP relay
- Configure the interface for QoS

Policy command mode

The Policy command mode is used to configure policies. To get access to Policy command mode, open the CLI in the Configuration command mode, then use the command **policy**. You can use Policy mode to perform these functions:

- Create and modify rules and schedules
- Manage user accounts
- Define users, groups, and aliases for use in policies
- Control branch office VPN gateways and tunnels
- Configure branch office and mobile user VPN policies

Common commands

Many commands are shared by all four command modes. These are known as “common commands”. In this Reference Guide, the common commands are in a separate chapter. You can use common commands in all four modes with all optional commands and parameters unless otherwise noted. The types of commands available in all command modes include:

- Help and history
- Commands to display settings, log messages, and status

Command Line Interface Prompt

The prompt displayed by the WatchGuard Command Line Interface (CLI) changes to reflect the working command mode.

Command Mode	Command Set	Prompt
Main (read write)	Common and Main commands	WG#
Main (read only)	Common and Main commands	WG>
Configuration	Common and Configuration commands	WG(config)#
Interface	Common and Interface commands	WG(config/if-fe0)#
Policy	Common and Policy commands	WG(config/policy)#

3 Common Commands

Common commands are those commands that are available in all four of the WatchGuard Command Line Interface (CLI) command modes. Any minor differences in the behavior of these commands due to the working command mode are described in each individual command mode chapter.

Due to the complexity of the **show** command, the reference for this command is divided into individual command mode references for each variant of this command.

List of Common Commands

These commands are available in all command modes:

Command	Usage
exit	In the Main mode, exit the CLI. Otherwise, return to the previous mode.
help	See general information or possible syntax for specified command.
history	See a list of the last 100 commands entered into the CLI.
show	Display information about a component of the current configuration or status.

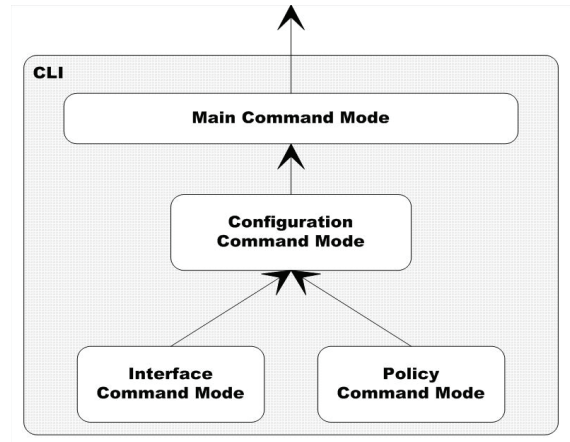
Common Command Reference

exit

Description: In the Main mode, exit the CLI. Otherwise, return to the previous mode.

Syntax:

exit
No options available.



help

Description: See general information or possible syntax for specified command. For more information, see “Get Help” on page 5.

Syntax:

help command
If no command provided, describes general features of the help system. If command provided, returns a list of all the possible syntaxes for the specified command. If ? provided for command, returns a list of all commands for which help is available in current command mode. command must be a valid command for the current command mode.

Example:

```

help arp
[1] arp (flush)

help diagnose
[1] diagnose [to(<ftp>|<tftp>)|cluster[to(<ftp>|<tftp>)]]
[2] diagnose vpn<ident>

help export
[1] export (blocked-site|allowed-site) to (<ftp>|<tftp>)
[2] export (config) to (<ftp>|<tftp>|console)
[3] export mvvpn <ident> to (<ftp>|<tftp>|console)
[4] export support to (<ftp>|<tftp>)

help ping
[1] ping <mstring>

help tcpdump
[1] tcpdump [<mstring>]*
    
```

history

Description: Display the command history list with line numbers.

Syntax:

history
Display commands entered into the CLI with line numbers.

Example:

```
history
```

show

Description: Display information about a component of the current configuration or status. Due to the complexity of the show command, individual components are detailed below.

Syntax:

show <i>component</i>
<i>component</i> must be a valid command. If ? is used for component, returns a list of all valid strings for <i>component</i> .

This table is a list of ***component*** values for which no options are available.

Component	Display
<i>arp</i>	ARP table
<i>auth-setting outbound-access-list</i>	List of IP addresses currently allowed outbound access, and shows the maximum number of allowed IP addresses (Firebox X Edge only)
<i>clock</i>	Manage the system clock
<i>default-packet-handling</i>	Default packet handling
<i>dynamic-nat</i>	Dynamic NAT
<i>factory-default</i>	Factory default configuration
<i>features</i>	Active licensed software features
<i>login-user</i>	List of management users logged on to the device
<i>managed-client</i>	Configure this device as a managed client
<i>network-mode</i>	WatchGuard security appliance system mode
<i>multi-wan</i>	Multiple wide area network settings
<i>ntp</i>	Network Time Protocol
<i>one-to-one-nat</i>	1-to-1 NAT settings for the device
<i>pptp</i>	Point-to-Point Tunneling Protocol
<i>proxy-action</i>	Default proxy actions
<i>route</i>	Established static routes
<i>signature-update</i>	Signature update configuration settings
<i>snmp</i>	Simple Network Management Protocol (SNMP) settings
<i>sslvpn</i>	Secure Sockets Layer Virtual Private Network
<i>static-arp</i>	Static ARP entries added to the static ARP table
<i>status-report</i>	Shows system status

Component	Display
<i>sysinfo</i>	Shows system information
<i>upgrade</i>	The audit trail of software upgrade(s)
<i>vpn-setting</i>	Global settings for virtual private networking
<i>vpn-status bovpn</i>	Active branch office VPN tunnels
<i>vpn-status pptp</i>	Active Mobile VPN with PPTP users

show cluster

Description: Display the names of FireCluster members or the status of the cluster.

Syntax:

show cluster component	
component is one of these options:	
<i>member</i>	Shows the list of FireCluster members
<i>status</i>	Shows the current status of the FireCluster

show ip

Description: Display the Internet Protocol settings for selected component.

Syntax:

show ip component	
component must be one of these options: <i>allowed-site</i> , <i>blocked-port</i> , <i>blocked-site</i> , <i>dns</i> , <i>dynamic-routing</i> , <i>route</i> , or <i>wins</i> .	

show log-setting

Description: Display the log settings for a specified component.

Syntax:

show log-setting component	
component is one of these options:	
Component	Description
<i>firebox-itself-logging</i>	Enable logging of traffic sent by the Firebox
<i>log-level</i>	Diagnostic log level
<i>ike-packet-trace</i>	IKE packet trace
<i>internal-storage</i>	Internal storage
<i>performance-statistics</i>	Performance statistics
<i>syslog-server</i>	Syslog server
<i>watchguard-log-server</i>	WatchGuard Log Server

show proposal

Description: Display the settings for the specified branch office VPN IPsec proposal.

Syntax:

show proposal <i>proposal number</i>
<i>p1</i> - Phase 1 proposal <i>p2</i> - Phase 2 proposal

show objects

Description: Use to display all the settings associated with a named object.

Syntax:

show object name	
<i>name</i> is the name of the object If <i>name</i> is not specified, a list of all configured objects of the type object appears object is one of these options:	
Object	Description
<i>alias</i>	Alias
<i>auth-server</i>	Authentication server
<i>auth-setting</i>	Authentication settings
<i>auth-user-group</i>	Authorized user and group
<i>bovpn-gateway</i>	Branch office virtual private network gateways
<i>bovpn-tunnel</i>	Branch office virtual private network tunnels
<i>feature-key</i>	WatchGuard feature key
<i>global-setting</i>	Global settings for the device
<i>mvpn-ipsec</i>	Mobile VPN with IPsec group configuration
<i>mvpn-rule</i>	Mobile VPN with IPsec policies
<i>policy-type</i>	Policy template
<i>rule</i>	Policy rule specification
<i>schedule</i>	Schedule to control traffic by time and day of week
<i>traffic-management</i>	Traffic management action
<i>user-group</i>	Firebox authentication user group
<i>users</i>	Firebox authentication user

show bridge

Description: Display the Bridge virtual interface configuration and status.

Syntax:

show bridge <i>bridgename</i>
<i>bridgename</i> is the virtual interface name. If <i>bridgename</i> is provided, the device displays information for only the specified virtual interface. Otherwise, it displays information for all configured bridge interfaces.

show certificate

Description: Display the certificates available in the WatchGuard device.

Syntax:

show certificate <i>component</i>	
<i>component</i> is one of these options:	
Component	Description
<cr>	Carriage return
<int>	Certificate ID <10000-99999>
<i>fingerprint</i>	Certificate fingerprint of a certificate on the device
<i>name</i>	Name of the entity
<i>type</i>	Show the certificates by type

show ddns

Description: Display the dynamic DNS service configuration information.

Syntax:

show ddns <i>type</i>
<i>type</i> is the dynamic DNS service type. The only valid string is <i>DynDNS</i> .

show interface

Description: Display the physical interface configuration and status.

Syntax:

show interface <i>number</i>
<i>number</i> is the network interface number. <i>number</i> must represent a valid number for the device. If <i>number</i> is provided, the device displays information for only the specified interface. Otherwise, it displays information for all interfaces.

show log-cache

Description: Display the internal temporary log repository for Traffic Monitor.

You can use the command options together to limit the entries that appear.

Syntax:

show log-cache
Display entire contents of the log cache.
show log-cache <u>sequence</u> <i>startpoint</i>
Display log entries from a specified start point of the log repository. <i>startpoint</i> is the starting sequence number of the log entries to include.
show log-cache <u>count</u> <i>number</i>
Limit the number of log entries to display. <i>number</i> is the maximum number of log entries to include. It must be an integer from 1 to 10000.
show log-cache <u>key</u> <i>pattern</i>
Display log entries that contain a pattern. <i>pattern</i> is the search key that must be present in the log cache for it to appear.

show log-cache tail <i>number</i>
Display log entries backward from the end of the internal log repository. <i>number</i> is the maximum number of log entries to include. It must be an integer from 1 to 10000.
show log-cache key <i>pattern</i>
Display entries that contain the key value specified in the <i>pattern</i> .

show usb

Description: Display information about the attached USB drive.

Syntax:

show usb
Show information about the USB drive attached to the device.
show usb flash-image
Show a list of saved backup image files stored on the USB drive.
show usb auto-restore
Show information about the auto-restore image stored on the USB drive.

show wireless

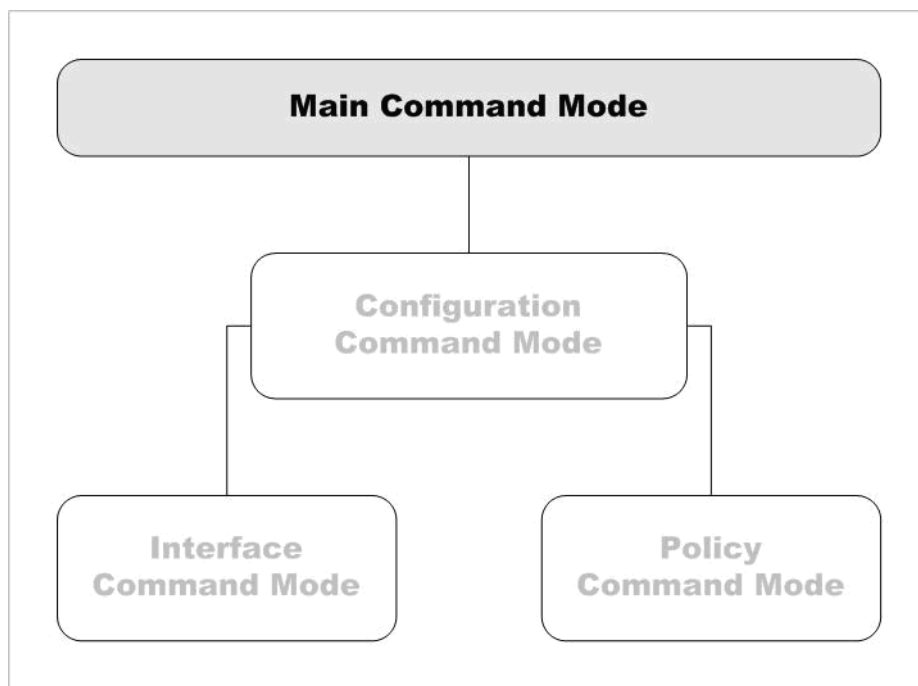
Description: Display the wireless settings and status for a WatchGuard wireless device.

Example:

show wireless ap <i>number</i>
Display the configuration for a wireless access point. <i>number</i> must be 1 or 2
show wireless client
Display the configuration of wireless client as an external interface.
show wireless guest
Display the configuration for the wireless guest network.
show wireless guest hotspot
Display the configuration for the wireless hotspot on the wireless guest network.
show wireless guest hotspot users
Display a list of wireless clients connected to your wireless hotspot.
show wireless status
Display the wireless network and radio settings.

4 Main Command Mode

The Main command mode is the default mode of the WatchGuard Command Line Interface (CLI).



In the Main mode, you can:

- Modify some higher level configuration settings
- Enter the Configuration command mode
- Restore or upgrade the software image
- Shut down or reboot the WatchGuard device

Enter the Main Command Mode

There are two methods to enter the Main command mode:

- Start the Command Line Interface
- Use the **exit** command while in the Configuration command mode

When you enter the Main mode, the prompt changes based on whether you connected to the device with the read-write admin account (WG#) or the read-only status account (WG>).

List of Main Mode Commands

You can use all common commands in the Main command mode. For more information, see “List of Common Commands” on page 15.

In addition, these commands are available only in the Main mode:

Command	Usage
arp flush	Clear the ARP cache of all entries.
backup image	Store a backup copy of the flash disk image.
cert-request	Use the WatchGuard device to create a security certificate.
checksum	Generate and display the MD5 checksum of all the packages installed.
clock	Manage and change the system clock.
configure	Enter the Configuration command mode.
debug-cli	Configure debugging options.
diagnose	Display internal diagnostic information.
dnslookup	Domain name resolution.
export	Export information to an external platform or file.
import	Import information from an external platform or file.
password	Change the administrator read-write or read-only password.
ping	Send a ping request to the specified IP address.
reboot	Stop all processing and do a cold restart of the device.
restore	Restore the device to a backup image or default configuration.
shutdown	Shut down the WatchGuard device.
sync	Retrieve the feature key, RSS feed, or XTM 2 Series wireless region for a WatchGuard device from the WatchGuard LiveSecurity server.
sysinfo	Display the WatchGuard device system information.
tcpdump	Dump traffic on the network.
traceroute	Examine and display the route to a specified destination.
upgrade	Upgrade the OS.
usb	Save a back up flash disk image or a diagnostic file to the USB drive attached to the device.
vpn-tunnel	Force the rekey of a BOVPN gateway.
who	Display a list of administrator users logged in to the WatchGuard device.

Main Command Mode Reference

arp flush

Description: Clear the ARP cache of all entries.

Syntax:

arp flush
No options available.

backup image

Description: Store a backup copy of the flash disk image.

Syntax:

backup image <i>password to location</i>
Store a backup copy of the flash disk image to an FTP or TFTP address. <i>password</i> is the password to use for this backup image. <i>location</i> must be a valid FTP or TFTP address.
backup image <i>password to usb filename</i>
Store a backup copy of the flash disk image to a USB drive attached to the device. <i>password</i> is the password to use for this backup image. <i>filename</i> is the name to use for the backup image file.

Example:

```
backup image readwritefoo to ftp://joez:passwd1@100.100.100.3/2010-05-12.fxi
backup image readwritefoo to usb 2010-05-12.fxi
```

cert-request

Description: Use the WatchGuard device to create a security certificate.

Syntax:

cert-request <i>purpose commonname companyname dnsname country countryname state statename city cityname department deptname address deviceaddress domain domain algorithm key-type length key-length usage key-usage</i>
<i>purpose</i> must be one of these options: https-proxy-authority, https-proxy-server, ipsec-web-server-other. <i>commonname</i> is the certificate common name. <i>companyname</i> is a string that identifies the issuer of the certificate. This should be your company name. <i>dnsname</i> is the fully qualified domain name. <i>countryname</i> is a string that identifies the country of origin, C. The default is US. <i>statename</i> is a string that identifies the state or province of origin, ST. <i>cityname</i> is a string that identifies the city or location of origin, L. <i>deptname</i> is a string that identifies the department of origin within a larger organization, OU. <i>deviceaddress</i> is an IP address that identifies the device of origin. <i>domain</i> is the domain name of the company of origin. <i>key-type</i> must be either <i>dsa</i> or <i>rsa</i> . The default is RSA. <i>key-length</i> must be either <i>length-1024</i> or <i>length-2048</i> <i>key-usage</i> is optional for ipsec-web-server-other only. If you use DSA encryption, the value must be <i>signature</i> . If RSA encryption, the value must be one of these options: <i>encryption</i> , <i>signature</i> , or <i>both</i> .

Example:

```
cert-request https-proxy-authority BigCompanyAcct BigCompany www.bigcom-  
pany.com country US  
cert-request https-proxy-server BigCompanyAcct BigCompany www.bigcompany.com  
country US state Maine department Accounting address 200.202.12.3 domain  
www.bigcompany.com algorithm dsa length 1024
```

checksum

Description: Generate and display the checksum of all the packages installed on the device.

Syntax:

checksum
No options available.

Example:

```
checksum
```

clock

Description: Manage and change the system clock.

Syntax:

clock time HH:MM:SS <u>date</u> MM/DD/YYYY
<i>time</i> is in the format: HH:MM:SS. The selection of AM or PM is not supported, thus the hours must be entered in the range 0 to 23.
<i>date</i> is in the format MM/DD/YYYY. Leading zeroes are not required in the month and day fields.

Example:

```
clock time 11:30:56 date 12/1/2004
```

configure

Description: Enter the Configuration command mode.

Syntax:

configure
No options available.

debug-cli

Description: Configure debugging options.

Syntax:

debug-cli <i>level</i>
<i>level</i> must be one of these options: <i>critical</i> , <i>error</i> , <i>warning</i> , <i>info</i> , <i>debug</i> , or <i>dump</i>

Example:

```
debug-cli critical
```

diagnose

Description: Display diagnostic information about a component. Because of the complexity of the diagnose command, individual components are detailed below.

Syntax:

diagnose *component*

Component must be a valid command parameter.

If ? is used for component, returns a list of all valid strings for ***component***.

diagnose to

Description: Specify an external location to send diagnostic information.

Syntax:

diagnose to *location*

Send diagnostic information of a device to an external location.

location must be either an FTP or TFTP address.

Example:

```
diagnose to tftp://bigcoftp/files/upload/memory.dot
```

diagnose cluster

Description: Display diagnostic information about a FireCluster.

Syntax:

diagnose cluster to *location*

Send diagnostic information for a cluster of WatchGuard devices to an external location.

location must be either an FTP or TFTP address.

Example:

```
diagnose cluster
```

diagnose hardware



The flash and memory diagnostics commands can affect system performance while the test runs.

Description: Perform diagnostic tests and display hardware diagnostic information for a WatchGuard XTM device. These commands do not apply to Firebox X e-Series devices. Some options do not apply to WatchGuard XTM 2 Series devices.

Syntax:

diagnose hardware ethernet nic-nums

Display the total number of ethernet interfaces on an XTM 5, 8, or 10 Series device.

diagnose hardware ethernet *option interface*

Display diagnostic information about an ethernet interface on an XTM 5, 8, or 10 Series device.

option must be one of these options:

- *nic-errors* — displays interface diagnostics error reports for the specified interface.
- *nic-stat* — displays the status of the specified interface.

interface must be a valid ethernet interface name on the device. For example, eth0.

diagnose hardware flash <i>partition size</i>
Perform a diagnostic check of the specified device partition for any XTM device. <i>partition</i> is the partition to test. It must be one of these options: <ul style="list-style-type: none"> - <i>boot</i> — The boot partition. - <i>sysa-data</i> — The system data partition - <i>sysa-kernel</i> — The Fireware XTM kernel partition (XTM 2 Series models only) - <i>sysa-program</i> — The Fireware XTM OS partition - <i>sysb-kernel</i> — The Fireware XTM kernel partition for system recovery (XTM 2 Series models only) - <i>sysb-program</i> — The Fireware XTM OS partition for system recovery <i>size</i> is the block size to use for the test. It must be an integer between 1 and 8; default is 2. The block size is multiplied by 512 for the test.
diagnose hardware memory <i>size number</i>
Perform diagnostic memory tests on available RAM for any WatchGuard XTM device. <i>size</i> is the block size, in kilobytes, to use for the test. <i>number</i> is the number of times to run the test. The default is 1. The block size for the test must be less than 10% of the free memory on the device. If you specify a block size that is too large, a message shows the free memory and maximum block size you can use.
diagnose hardware system
Display the CPU temperature, fan speed, and voltage for an XTM 5, 8, or 10 Series device.

Example:

```
diagnose hardware ethernet nic-nums
diagnose hardware ethernet nic-stat eth0
diagnose hardware system
diagnose hardware flash boot
diagnose hardware memory 500
```

diagnose vpn**Description:** Display diagnostic information for configured VPNs.**Syntax:**

diagnose vpn <i>"/ike/pktrace/set number"</i>
Set the VPN diagnostic packet trace level of a device. <i>number</i> must be one of these options: 0:off, 1:start and overwrite, 2:rotate, 3:append, 4:reset.
diagnose vpn <i>"/ike/counters"</i>
Display the VPN diagnostic global counters.
diagnose vpn <i>"/ike/restart"</i>
Restart the Internet Key Exchange of the VPN.
diagnose vpn <i>"/ike/gateway/list"</i>
Display the list of the configured gateways of a device.
diagnose vpn <i>"/ike/gateway/info gw-name"</i>
Display detailed information for the specified gateway. <i>gw-name</i> is the specific gateway to be displayed.
diagnose vpn <i>"/ike/policy/list"</i>
Display the configured IKE policy list of a device.

diagnose vpn <i>"/ike/policy/info ike-pol-name"</i>
Display detailed information for the specified IKE policy. <i>ike-pol-name</i> is the specific IKE policy to be displayed.
diagnose vpn <i>"/ike/policy/conn ike-pol-name"</i>
Start a Phase 1 negotiation for the specified IKE policy. <i>ike-pol-name</i> is the specific IKE policy to be negotiated.
diagnose vpn <i>"/ike/policy/counters ike-pol-name"</i>
Display the counters for the specified IKE policy. <i>ike-pol-name</i> is the specific IKE policy to be displayed.
diagnose vpn <i>"/ike/sa/list"</i>
Display the established Phase-1 SA list from all the internal hash tables.
diagnose vpn <i>"/ike/sa/list/policy"</i>
Display the Phase-1 SA list from a single hash table.
diagnose vpn <i>"/ike/sa/counters hash-id initcookie respcookie"</i>
Display the Phase-1 SA counter information. <i>hash-id</i> is the hash index. <i>initcookie</i> is the initiator cookie. <i>respcookie</i> is the responder cookie. All of these parameters can be obtained from diagnose vpn <i>"/ike/sa/list"</i> command.
diagnose vpn <i>"/ipsec/policy/list"</i>
Display the configure IPSec policy list.
diagnose vpn <i>"/ipsec/policy/info ipsec-pol-name"</i>
Display the detailed information of the specified IPSec policy. <i>ipsec-pol-name</i> is the specific IPSec policy to be displayed.
diagnose vpn <i>"/ipsec/policy/rinfo"</i>
Display the information about IPSec policies.
diagnose vpn <i>"/ipsec/policy/rinfo ike_policy gw-name"</i>
Display the information about IPSec policies that are in the specified IKE policy. <i>gw-name</i> is the gateway name.
diagnose vpn <i>"/ipsec/policy/rinfo ipsec_policy tnl-name"</i>
Display the information about the specified IPSec policy. <i>tnl-name</i> is the tunnel name.
diagnose vpn <i>"/ipsec/sa/list"</i>
Display all available IPSec SAs.
diagnose vpn <i>"/ipsec/sa/list ike_policy gw-name"</i>
Display all IPSec SA for the specified IKE policy. <i>gw-name</i> is the gateway name.
diagnose vpn <i>"/ipsec/sa/list ipsec_policy tnl-name"</i>
Display all IPSec SA for the specified IPSec policy. <i>tnl-name</i> is the tunnel name.
diagnose vpn <i>"/ipsec/sa/list cluster_id id"</i>
Display all IPSec SA for the specified Cluster ID. <i>id</i> is the Cluster ID. Use the diagnose vpn <i>"/ipsec/sa/list"</i> command to get the ID.

diagnose vpn <i>"/ipsec/sa/list local num"</i>
<i>num</i> is one of these options: <ul style="list-style-type: none"> - "0" to display all IPsec SA including SAs of other cluster members - "1" to display all IPsec SA local to the box.
diagnose vpn <i>"/ipsec/sa/ikepcy/list ike_policy gw-name"</i>
Display all IPsec SA for the specified IKE policy. <i>gw-name</i> is the gateway name.
diagnose vpn <i>"/ipsec/sa/ipsecpcy/list"</i>
Display all IPsec SA for the specified IPsec policy.
diagnose vpn <i>"/ipsec/sp/list"</i>
Display all available security policies.
diagnose vpn <i>"/ipsec/sp/list ike_policy gw-name"</i>
Display all security policies for the specified IKE policy. <i>gw-name</i> is the gateway name.
diagnose vpn <i>"/ipsec/sp/list ipsec_policy tnl-name"</i>
Display all security policies for the specified IPsec policy. <i>tnl-name</i> is the tunnel name.
diagnose vpn <i>"/ipsec/sp/info dir direction index idx"</i>
Display detailed information about the specified security policy. <i>direction</i> can be either "in", "out" or "fwd". <i>index</i> is Security Policy index. Use the diagnose vpn <i>"/ipsec/sp/list"</i> command to get both of these parameters.
diagnose vpn <i>"/ipsec/counters"</i>
Display global level encryption/decryption packet and bytes counts.
diagnose vpn <i>"/ipsec/spi/hashtable"</i>
Display entries in IKE's SPI hash table.
diagnose vpn <i>"/ipsec/cluster/topology"</i>
Display cluster topology information.
diagnose vpn <i>"/ipsec/bovpn/rekey"</i>
Initiate Phase-2 rekey for all available BOVPN tunnels.
diagnose vpn <i>"/ipsec/bovpn/rekey gateway gw-name"</i>
Initiate Phase-2 rekey for all the Tunnels for the specified Gateway. <i>gw-name</i> is the gateway name.
diagnose vpn <i>"/ipsec/bovpn/rekey ipsec_policy tnl-name spi in p2said-in spi out p2said-out"</i>
Initiate Phase-2 rekey for the specified Tunnel. If Phase-2 ID for either Inbound or Outbound, or both, are specified, only those will have a rekey. <i>tnl-name</i> is the tunnel name. <i>p2said-in</i> is the Inbound Phase-2 SA ID. <i>p2said-out</i> is the Outbound Phase-2 SA ID. Use diagnose vpn <i>"/ipsec/policy/rtinfo"</i> to get the <i>p2said-in</i> and <i>p2said-out</i> parameters.

Example:

```
diagnose vpn "/ike/sa/list"
diagnose vpn "/ike/tracelevel/set 2"
diagnose vpn "/ipsec/bovpn/rekey ipsec_policy tunnel.1 spi_in 0x349c2b2"
```

dnslookup

Description: Look up domain name.

Syntax:

dnslookup <i>domainname</i>
Resolve a domain name. <i>domainname</i> must be a Fully Qualified Domain Name (FQDN).

Example:

```
dnslookup www.companyname.com
```

export

Description: Export information to an external platform or file.

Syntax:

export <i>type</i> to <i>location</i>
Export the blocked sites or allowed sites list to a file. <i>type</i> must be one of these options: <i>blocked site</i> or <i>allowed-site</i> <i>location</i> must be either an FTP or TFTP address.
export <u>config</u> to <i>location</i>
Export the XTM device configuration to a file. <i>location</i> must be either an FTP, TFTP address or console.
export <u>muvpn</u> <i>muvpnid</i> <u>client-type</u> <i>client</i> to <i>location</i>
Export the Mobile VPN with IPsec client configuration to a file. <i>muvpnid</i> must be an existing Mobile VPN with IPsec group. <i>client</i> must be one of these options: <i>watchguard</i> or <i>shrew-soft-client</i> . - <i>watchguard</i> — export the .ini profile for use with the WatchGuard Mobile VPN with IPsec client. - <i>shrew-soft-client</i> — export the .vpn profile for use with the Shrew Soft VPN client. <i>location</i> must be either an FTP, TFTP address or console.
export <u>support</u> to <i>location</i>
Export support information to a file. <i>location</i> must be either an FTP or TFTP address.

Example:

```
export blocked-site to ftp://joez:1pass@ftp.bigco.com:23/upload/blocked.dot
export muvpn ipsec-users client-type shrew-soft-client to ftp://
joez:1pass@ftp.bigco.com:23/upload/ipsec-users.vpn
```

import

Description: Import information from an external platform or file.

Syntax:

import type action option from location
<i>type</i> must be one of these options: <i>blocked-site</i> or <i>allowed-site</i> . <i>option</i> must be one of these options: <i>override</i> or <i>merge</i> . <i>location</i> must be either an FTP or TFTP address.
import type from location
<i>type</i> must be one of these options: <i>bulk-license</i> , <i>certificate</i> , <i>crl</i> , <i>config</i> or <i>feature-key</i> . <i>location</i> must be either an FTP or TFTP address.
import route-config type from location
<i>type</i> must be one of these options: <i>bgp</i> , <i>rip</i> , or <i>ospf</i> . <i>location</i> must be either an FTP or TFTP address or <i>console</i> .

Example:

```
import blocked-site action merge from tftp://myftpsite/files/upload/site.dot
import certificate from tftp://myftpsite/files/upload/cert.dot
import bulk-license from tftp://myftpsite/files/upload/keys.dot
import route-config ospf from console
```

password

Description: Change the administrator read-write or read-only password.

Syntax:

password
No options available.

ping

Description: Send a ping request to the specified IP address.

Syntax:

ping <mstring> host
<i>host</i> is the host name or IP address in the format A.B.C.D.

Example:

```
ping 74.125.19.147
ping -c 5 74.125.19.147
```

reboot

Description: Stop all processing and do a cold restart of the device.

Syntax:

reboot
No options available.

restore

Description: Restore the device to a backup image or default configuration.

Syntax:

restore factory-default
Restore the device to its factory default configuration. No options available.
restore image from <i>location</i> <i>password</i>
<i>location</i> is a valid FTP or TFTP address. <i>password</i> is the restore password of the backup image file.
restore image from USB <i>imagetype</i> <i>imagename</i> <i>password</i>
<i>imagetype</i> is the type of image to restore. It must be one of these options: <ul style="list-style-type: none"> - <i>auto-restore</i> — restore the auto-restore image - <i>flash image</i> — restore any backup image <i>imagename</i> is the file name of the backup image. <i>password</i> is the restore password of the backup image file.

Example:

```
restore image from tftp://myftpsite/files/upload/april.fxi configpasswordfoo
restore image from usb flash-image 2012-02-01.fxi configpasswordfoo
```

shutdown

Description: Shut down the WatchGuard device.

Syntax:

shutdown
No options available.

sync

Description: Retrieve the feature key, RSS feed, or XTM 2 Series wireless region from the WatchGuard LiveSecurity server. The RSS feed is available from the LiveSecurity® Service.

Syntax:

sync feature-key <u>apply</u>
<u>apply</u> causes the WatchGuard device to use the updated feature key immediately. If you do not use the <u>apply</u> option, the WatchGuard device does not use the new feature key until you reboot the device.
sync rss-feed
No options available.
sync wireless
No options available. Applies to XTM 2 Series wireless models only.

Example:

```
sync feature-key apply
sync wireless
```

sysinfo

Description: Display the WatchGuard device system information.

Syntax:

sysinfo
No options available.

tcpdump

Description: Dump traffic on the network.

Syntax:

tcpdump <u><mstring></u>
No options available.

Example:

```
tcpdump -d -q
```

traceroute

Description: Examine and display the route to a specified destination.

Syntax:

traceroute <u><mstring></u> <i>host</i>
<i>host</i> is a valid IP address.

Example:

```
traceroute -d 74.125.19.147
```

upgrade

Description: Upgrade the OS.

Syntax:

upgrade system from <i>location</i> <u>force</u>
<i>location</i> must be either an FTP or TFTP address. <u>force</u> must be one of these options: <i>yes</i> or <i>no</i> . This forces the system upgrade.

Example:

```
upgrade system from ftp://test:testing@1.2.3.4/upg.wgu yes
```

usb

Description: Format an attached USB drive and manage backup image files on the USB drive.

usb format
Format the USB drive attached to the device as a FAT32 partition.
usb auto-restore <i>password filename</i>
Select a saved backup image on the USB drive to use as the image for auto-restore. <i>password</i> is the password used to encrypt the backup image. <i>filename</i> is the filename of the saved backup image. To create the backup image file, use the backup image command.
no usb auto-restore
Delete the auto-restore image from the USB drive.
no usb image <i>filename</i>
Delete a saved backup image from the USB drive.

Example:

```
usb format
usb auto-restore mypassw0rd 2010-04-29.v11.3.fxi
no usb auto-restore
no usb image 2010-04-20.v11.2.fxi
```

vpn-tunnel

Description: Force the rekey of a BOVPN gateway.

Syntax:

vpn-tunnel rekey <i>gateway</i>
<i>gateway</i> identifies a BOVPN gateway.

Example:

```
vpn-tunnel rekey ChicagoSeattle
```

who

Description: Display a list of administrator users logged in to the WatchGuard device.

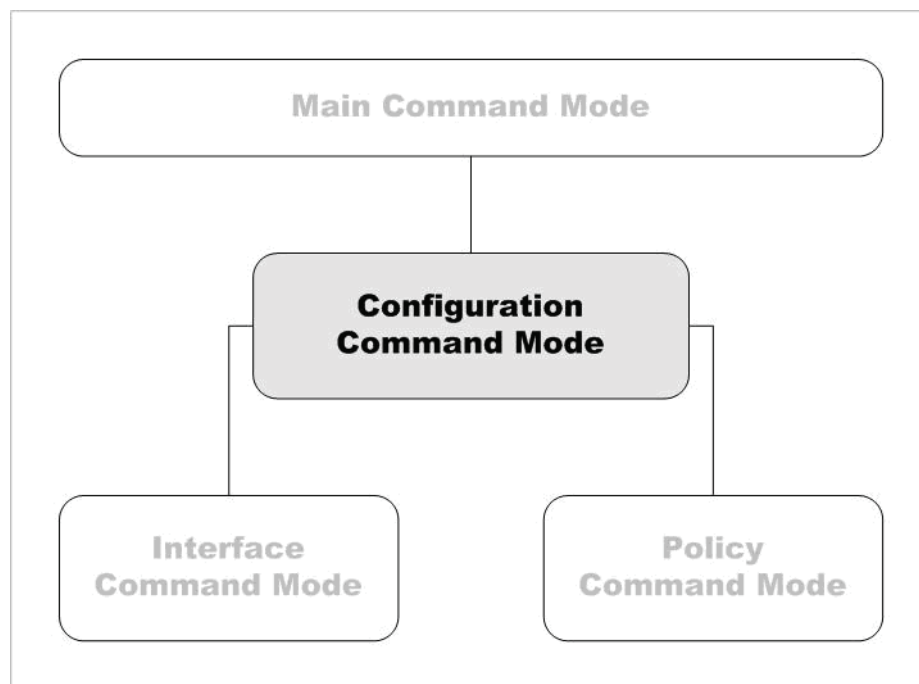
Syntax:

who
No options available.

5

Configuration Command Mode

The WatchGuard Command Line Interface (CLI) Configuration command mode is used for system and network configuration of your Firebox or XTM device.



In the Configuration mode, you can:

- Manage user accounts
- Manage the logging performed by the WatchGuard device
- Configure global network settings
- Control branch office VPN gateways and tunnels
- Enter the Policy and Interface command modes

Enter the Configuration Command Mode

There are two methods to enter the Configuration command mode:

- Use the **configure** command while in the Main command mode
- Use the **exit** command while in the Policy or Interface command modes.

When you get access to the Configuration command mode, the CLI prompt changes to `wg(config)#`.

List of Configuration Mode Commands

You can use all common commands in the Configuration command mode. For more information, see “List of Common Commands” on page 15.

In addition, these commands are available only in the Configuration mode:

Command	Usage
auth-setting	Configure settings for authentication.
bridge	Assign a name to a VLAN bridge.
cluster	Configure settings for FireCluster.
ddns	Configure settings for dynamic DNS.
default-packet-handling	Configure the default packet handling settings.
global-setting	Configure the global settings of a device.
interface	Enter the Interface command mode for the specified interface.
ip	Configure IP settings for firewall features such as block sites and ports.
ldap	Configure the device to use an LDAP authentication server.
log-setting	Define how and where the device sends log messages.
managed-client	Configure the device to be a managed client.
multi-wan	Configure the device with multiple external interfaces.
network-mode	Change the system configuration mode to either Mixed Routed, Drop-in, or Bridge.
ntp	Configure the device to use an NTP server.
policy	Enter the Policy command mode.
signature-update	Configure updates to IPS and Gateway AV signatures files and engine.
snmp	Configure the device to interoperate with SNMP tools.
static-arp	Hard code a static-arp binding.
system	Set the system properties.
vlan	Create VLAN interface on the device.
vpn-setting	Configure global VPN settings
web-server-cert	Configure the web server certificate to use for Firebox authentication.
wireless	Configure Wi-Fi settings. For Firebox X Edge e-Series and XTM 2 Series wireless devices only.

Configuration Command Mode Reference

auth-setting

Description: Configure the authentication service of the device.

Syntax:

auth-setting timeout-type day <i>days</i> hour <i>hours</i> minute <i>minutes</i> second <i>seconds</i>
Configure the timeout setting options for authentication. timeout-type is the authentication option that must be set for timeout. It must be one of these options: <i>auth-user-idle-timeout</i> , <i>auth-user-session-timeout</i> , <i>mgmt-user-idle-timeout</i> , or <i>mgmt-user-session-timeout</i> . <i>days</i> is the duration in days. It must be an integer from 0 to 365. <i>hours</i> is the duration in hours. It must be an integer from 0 to 23. <i>minutes</i> is the duration in minutes. It must be an integer from 0 to 59. <i>seconds</i> is the duration in seconds. It must be an integer from 0 to 59.
auth-setting auto-redirect enable
Automatically redirect the user to the authentication page for authentication.
auth-setting auto-redirect url <i>url-path</i>
Send a redirect to a particular web site to the browser after successful authentication. url-path is the web site to redirect after authentication.
no auth-setting outbound-access-list <i>ip-address</i>
Remove an IP address from the outbound access list. (Firebox X Edge e-Series models only.) ip-address is the IP address to remove from the list. It must be in the format A.B.C.D.
auth-setting outbound-access-list flush
Remove all IP addresses from the outbound access list. (Firebox X Edge only.)
auth-setting same-user-multi-login <i>setting</i>
Set authentication to allow or deny multiple logins from a user at the same time. For all WatchGuard device models except Firebox X Core e-Series: setting must be one of these options: 0 — Log off the first session when the user logs in a second time 1 — Allow multiple sessions for a user 2 — Reject subsequent log in attempts when a user is already logged in Set to 1 by default. For Firebox X Core e-Series models: setting must be one of these options: <i>enable</i> or <i>disable</i> . Set to <i>enable</i> by default.
auth-setting single-sign-on enable
Enable Single Sign-On (SSO) on the device. Use no auth-setting single-sign-on enable to disable SSO.
auth-setting single-sign-on agent <i>address</i> <i>cache -timeout</i>
Specify Single Sign-On (SSO) Agent on the network. address is the IP address of SSO Agent. cache-timeout is the amount of time in seconds the SSO information is stored.
auth-setting single-sign-on except-ip <i>ip-address</i> <i>ip-address</i>
Add SSO exception list. ip-address is the IP address of the computer to exempt from SSO. You can specify multiple IP addresses in the command.

Example:

```
auth-setting auth-user-idle-timeout minute 15
auth-setting mgmt-user-idle-timeout day 1 hour 6 minute 30
auth-setting auto-redirect enable
auth-setting auto-redirect url http://authsuccess.company.com/welcome/
auth-setting same-user-multi-login 2
auth-setting single-sign-on enable
auth-setting single-sign-on agent 10.0.1.253
auth-setting single-sign-on except-ip 10.0.1.33 10.0.1.55
```

bridge

Description: Create or edit a Bridge virtual interface on the device.

Syntax:

bridge <i>bridgename</i>
<i>bridgename</i> is a string that uniquely identifies the bridge. Use <u>no</u> bridge <i>bridgename</i> to delete the bridge virtual interface.

After you enter the command **bridge *bridgename*** the configuration continues to the Bridge details command. The prompt changes to "wG(config/bridge-*bridgename*)#". Use the **Exit** command to exit this mode.

security-zone <i>zone ip-address member if-number if-number if-number</i>
<i>zone</i> is the security zone. It must be either trusted or optional. <i>ip-address</i> is the IP address assigned to the virtual interface. It is either an address with a mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/#, where # must be in the range of 8 to 30. <i>if-number</i> is the interface index that is assigned as a member of the Bridge. You can specify more than two member interfaces of the Bridge.

Example:

```
bridge Bridge10
security-zone trusted 10.10.1.1/24 member 3 4 5
```

cluster

Description: Configure the FireCluster settings. This command does not apply to Firebox X Edge or XTM 2 Series devices.

Syntax:

cluster enable
Enable FireCluster feature of a device.
cluster id <i>c-id</i>
Set the identification number of a FireCluster. <i>c-id</i> is an identification number from 1 to 255.
cluster interface <i>if-type if-number</i>
Identifies the type and its corresponding interface of a FireCluster. <i>if-type</i> must be one of these options: <i>management</i> , <i>primary</i> , <i>secondary</i> . <i>if-number</i> is the interface number assigned to the specified type.

cluster mode <i>c-mode</i>
Selects the FireCluster mode. <i>c-mode</i> must be one of these options: <i>active-active</i> or <i>active-passive</i> .
cluster load-balance <i>type</i>
Specify the load balancing algorithm of an active/active FireCluster. <i>type</i> must be one of these options: <ul style="list-style-type: none"> - <i>Least-Connections</i> — Each new connection is assigned to the active cluster member with the lowest number of open connections. This is the default setting. - <i>Round-Robin</i> — New connections are distributed among the active cluster members in round-robin order. The first connection goes to one cluster member. The next connection goes to the other cluster member, and so on.
cluster member <i>option member-name serial-no primary-ip mgt-ip secondary-ip from source</i>
Add a new FireCluster member or edit an existing FireCluster member. <i>option</i> must be one of these options: <i>add</i> or <i>edit</i> . <i>member-name</i> is a string that is the name of the FireCluster member device. <i>serial-no</i> is the serial number of the device. <i>primary-ip</i> is the IP address of the primary FireCluster interface. <i>mgt-ip</i> is the management IP address of the FireCluster. <i>secondary-ip</i> is the IP address of the optional secondary FireCluster interface. <i>source</i> FireCluster member license file from one of these options: <i>FTP</i> , <i>TFTP</i> or <i>console</i> .
cluster notification snmp-trap enable
Activate and send SNMP traps for FireCluster.
cluster notification notification enable action-type <i>a-type</i> <u>launch-interval</u> <u>int</u> <u>repeat-count</u> <u>count</u>
Activate email or pop-up window notifications for FireCluster. <i>a-type</i> must be one of these options: <i>email</i> or <i>pop-window</i> . The default is email. <u>int</u> is the launch interval between 1 to 65535. The default is 15. <u>count</u> is the launch interval between 1 to 256. The default is 10.

Example:

```

cluster enable
cluster encryption encrypt-key
cluster id 3
cluster interface management 1
cluster member add Master 9085046373F7B 10.0.1.10/24 10.0.1.2/24 10.0.1.20/24
from ftp://ftp.company.com/licenses/9085046373F7B-license.txt
cluster mode active-active
cluster load-balance least-Connections
cluster notification snmp-trap enable
cluster notification notification enable action-type email launch-interval 20
repeat-count 5
    
```

ddns

Description: Configure the device to use a dynamic domain name service provider.

Syntax:

ddns DynDNS interface username password domainname *interval* *type* *options*

interface is the name of the interface configured to use DynDNS.
username is a string that represents the DynDNS user name.
password is the DynDNS password.
domainname is a string that is the domain name used for your DynDNS account.
interval is the time interval, in days, to force an update of the IP address. This must be an integer.
type is the DynDNS service type. It must be one of these options: *dyndns*, or *custom*.
options is a string composed of one or more DynDNS options:

- You must type the "&" character before and after each option you add.
- If you add more than one option, you must separate the options with the "&" character.
- Available options are: mx=mailexchanger, backmx=YES|NO, wildcard=ON|OFF|NOCHG, and offline=YES|NO

Example:

```
ddns DynDNS interface 0 watchguard strongpass2 watchguard.com 28 dyndns
"&backmx=NO&wildcard=ON&"
```

default-packet-handling

Description: Configure default packet handling settings.

Syntax:

default-packet-handling logging *type* *action* *logging-action* *launch-interval* *int* *repeat-count* *count*

Configure log settings for default packet handling options.

type is the type of log message to enable. It must be one of these options: *ip-spoofing*, *arp*, *port*, *address*, *ip-src*, *ping*, *ipsec*, *ike*, *syn*, *icmp*, *udp*, *ddos-des*, *ddos-src*, *incoming*, *outgoing*, *internal*, or *external*.

Use **no default-packet-handling logging category *type*** to disable the logging of packets of the specified category.

type is the form of notification. It must be one of these options:

- 1 is Send Log Message.
- 2 is Send SNMP trap
- 3 is Send Notification.

If the **type** selected is 3, these options are also available:

- *int* is the minimum time in minutes between notifications. It must be an integer from 1 to 65525.
- *count* is the number of times an event must occur before a repeat notification is sent. It must be an integer from 1 to 256.

default-packet-handling unhandled *option* enable

Set action taken for packets that do not match any default packet handling rule.

option is the action taken when the device receives a packet that does not match any rule. It must be one of these options: *auto-block* or *send-message*.

Use **no default-packet-handling unhandled** to disable all actions for unhandled packets.

default-packet-handling dangerous-active <i>activity</i> enable <i>threshold</i>
<p>Enable default packet handling rules for certain types of dangerous activity.</p> <p><i>activity</i> is the form of dangerous activity. It must be one of these options: <i>icmp-flood enable</i>, <i>syn-flood enable</i>, <i>udp-flood enable</i>, <i>ipsec-flood enable</i>, <i>ike-flood enable</i>, <i>ip-scan enable</i>, <i>port-scan enable</i>, <i>spoofing-attack enable</i>, or <i>source-route enable</i>.</p> <p><i>threshold</i> is the threshold value. It is an integer as follows:</p> <ul style="list-style-type: none"> - Ports 10 to 65535 for <i>icmp-flood</i> or <i>syn-flood</i>. - Packets per second 1 to 65535 for <i>udp-flood</i>, <i>ipsec-flood</i>, <i>ike-flood</i>, <i>ip-scan</i>, or <i>port-scan</i>. - Keep blank for <i>spoofing-attack</i> or <i>source-route enable</i>.
default-packet-handling ddos <i>side</i> enable <i>quota</i>
<p>Configure evaluation of traffic for DDoS.</p> <p><i>side</i> is whether to monitor based on the source or destination. It must be one of these options: <i>server-ddos</i> or <i>client-ddos</i>.</p> <p><i>quota</i> is the number of connections per second. It must be an integer from 10 to 65535.</p>

Example:

```
default-packet-handling logging ike 3 action 3 launch-interval 50 repeat-count 10
default-packet-handling unhandled auto-block enable
default-packet-handling dangerous-activity ike-flood enable 1000
default-packet-handling ddos server-ddos enable 1500
```

global-setting

Description: Define the global settings of the device.

Syntax:

global-setting auto-reboot enable
<p>Enable the auto-reboot feature for the device.</p> <p>Use <u>no</u> global-setting auto-reboot enable to disable auto-reboot.</p>
global-setting auto-reboot hour <i>hr</i> minute <i>min</i>
<p>Defines the auto-reboot timer for the device.</p> <p><i>hr</i> is the number of hours from 0 to 23.</p> <p><i>min</i> is the optional number of minutes from 0 to 59.</p>
global-setting icmp-message <i>message</i>
<p>Define the ICMP error message for the device.</p> <p>Use <u>no</u> global-setting icmp-message <i>message</i> to disable icmp-message function.</p> <p><i>message</i> is the ICMP message returned to the source. It must be one of these options: <i>allow-all</i>, <i>deny-all</i>, <i>fragmentation-required</i>, <i>host-unreachable</i>, <i>network-unreachable</i>, <i>port-unreachable</i>, <i>protocol-unreachable</i>, <i>time-exceeded</i>.</p> <p>If the <i>message</i> selected is <i>fragmentation-required</i>, then DF bit is set to 1.</p>
global-setting tcp-mss-adjustment <i>option</i>
<p>Set the maximum segment size adjustment.</p> <p><i>option</i> must be one of these options: <i>automatic</i> or limit-to <i>size</i></p> <ul style="list-style-type: none"> - <i>size</i> is the specified size in bits. It must be an integer from 40 to 1460.
global-setting tcp-syn-checking enable
<p>Enable the TCP/syn check for the device.</p> <p>Use <u>no</u> global-setting tcp-syn-checking enable to disable TCP/syn checking.</p>

global-setting traffic-management enable
Enable traffic management for the device. Use no global-setting traffic-management enable to disable traffic management for the device.
global-setting tcp-connection-timeout <i>unit</i> <i>timeout-value</i>
Set the TCP connection idle timeout value. <i>unit</i> is the time unit for the <i>timeout-value</i> . It must be one of these options: <i>day, hour, minute, second</i> . You can specify more than one <i>unit</i> , followed by the <i>timeout-value</i> for that unit. <i>timeout-value</i> is the connection timeout value associated with the timeout unit. Default idle timeout is 1 hour. Maximum idle timeout is 30 days.
global-setting webui-port <i>port</i>
Set the Web User Interface port for the device. <i>port</i> is the port number from 1 to 65535.

Example:

```
global-setting auto-reboot enable
global-setting auto-reboot hour 2 30
global-setting icmp-message deny-all
global-setting tcp-syn-checking enable
global-setting tcp-mss-adjustment automatic
global-setting tcp-mss-adjustment limit-to 100
global-setting traffic-management enable
global-setting tcp-connection-timeout hour 5 minute 30 seconds 10
global-setting webui-port 3128
```

interface

Description: Enter the Interface command mode for the specified interface.

Syntax:

interface FastEthernet <i>number</i>
<i>number</i> must be an integer from 0 to the max number of ports minus one, depending on the platform and model.

Example:

```
interface FastEthernet 0
WG(config/if-fe0)#
```

ip

Description: Configure Internet Protocol settings for firewall features, for example, block sites and ports.

Syntax:

ip allowed-site <i>address</i>
<p>Add or remove an address from the allowed IP address list.</p> <p><i>address</i> must be one of these options: <i>host ip</i>, <i>subnet net</i>, or <i>range startip endip</i>.</p> <ul style="list-style-type: none"> - <i>ip</i>, <i>startip</i>, and <i>endip</i> must be an IP address in the format of A.B.C.D. - <i>net</i> must be an IP subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32. <p>Use no ip allowed-site to clear all entries on the allowed IP address list.</p>
ip blocked portblocked-port port log logstate auto-blocked autostate alarm alarmsetting alarmoption
<p>Block all traffic to the specified port or ports.</p> <p>port is an integer from 1 to 65535. You can configure more than one port.</p> <p><i>logstate</i> enables or disables log messages when packets are addressed to the specified port. The value must be: <i>enable</i> or <i>disable</i>.</p> <p><i>autostate</i> enables automatic addition of the source IP address to the list of blocked sites when packets are addressed to the specified port. The value must be: <i>enable</i> or <i>disable</i>.</p> <p><i>alarmsetting</i> selects the notification alarm parameter. <i>alarmoption</i> configures the parameter. The values must be one of these options:</p> <ul style="list-style-type: none"> - <i>blocked-ip-enable</i> — <i>enable</i> or <i>disable</i> - <i>remote-enable</i> — <i>enable</i> or <i>disable</i> - <i>trap-enable</i> — <i>enable</i> or <i>disable</i> - <i>launch-interval</i> — an integer from 60 to 3932100 - <i>repeat-count</i> — an integer from 1 to 256 - <i>action-type</i> — <i>email</i> or <i>popup</i> <p>You can configure more than one alarm setting.</p>
ip blocked-site domain alarm alarmsetting alarmoption
<p>Block all traffic from the specified domain name.</p> <p>domain is a domain name, for DNS lookups</p> <p><i>alarmsetting</i> selects the notification alarm parameter. <i>alarmoption</i> configures the parameter. The value must be one of these options:</p> <ul style="list-style-type: none"> - <i>action-type</i> — the method for notification; <i>email</i> or <i>popup</i> - <i>blocked-ip-enable</i> — <i>enable</i> or <i>disable</i> - <i>launch-interval</i> — interval, in minutes; an integer from 60 to 3932100 - <i>remote-enable</i> — <i>enable</i> or <i>disable</i> - <i>repeat-count</i> — the repeat count; an integer from 1 to 256 - <i>trap-enable</i> — <i>enable</i> or <i>disable</i> <p>You can configure more than one alarm setting.</p>
ip blocked-site duration minutes
<p>Configure the duration that a site remains on the blocked sites list after being automatically added because of packet handling rules.</p> <p>minutes is an integer from 1 to 99999.</p>
ip blocked-site dynamic ip-address expire-after day dd hour hh minute min second sec
<p>Block all traffic from specified IP addresses for the specified time.</p> <p>ip-address is the host to be temporarily blocked.</p> <p><i>dd</i> is the number of days from 0 to 365.</p> <p><i>hh</i> is the number of hours from 0 to 23.</p> <p><i>min</i> is the number of minutes from 0 to 59.</p> <p><i>sec</i> is the number of seconds from 0 to 59.</p>

ip blocked-site dynamic flush
Flush the status of all dynamically blocked sites.
ip blocked-site address alarm <i>alarmsetting alarmoption</i>
Block all traffic from specified host, subnet or range of IP addresses. address must be one of these options: <i>host ip, subnet net, or range startip endip</i> . <ul style="list-style-type: none"> - <i>ip, startip, and endip</i> must be an IP address in the format of A.B.C.D. - <i>net</i> must be an IP subnet in the format of A.B.C.D/# where # must be in the range of 0 to 32. <i>alarmsetting</i> selects the notification alarm parameter. <i>alarmoption</i> configures the parameter. The value must be one of these options: <ul style="list-style-type: none"> - <i>blocked-ip-enable</i> — <i>enable</i> or <i>disable</i> - <i>remote-enable</i> — <i>enable</i> or <i>disable</i> - <i>trap-enable</i> — <i>enable</i> or <i>disable</i> - <i>launch-interval</i> — an integer from 60 to 3932100 - <i>repeat-count</i> — an integer from 1 to 256 - <i>action-type</i> — <i>email</i> or <i>popup</i> You can configure more than one alarm setting.
ip dns domain-name <i>domain</i>
Provide a default domain name to complete unqualified host names. domain is the provided domain name. Use <u>no</u> ip dns domain-name to remove the DNS domain name.
ip dns forwarding enable
Enable DNS forwarding. Use <u>no</u> ip dns forwarding enable to disable DNS forwarding.
ip dns server address
Add or remove a DNS server(s). address is the IP address of a DNS server. You can configure a maximum of three IP addresses. Use <u>no</u> ip dns servers to remove all DNS server entries.
ip dynamic-routing type
Set routing protocol. type must be one of these options: <i>bgp, ospf, or rip</i> .
ip route option fwdaddr metric <i>metricvalue</i>
Create a static network route. option must be one of these options: <i>address</i> or <i>net</i> . <ul style="list-style-type: none"> - <i>address</i> is the IP address for the destination in the format of A.B.C.D. - <i>net</i> is the IP subnet for the destination in the format of A.B.C.D/# where # must be in the range of 0 to 32. fwdaddr is the forwarding router's address in the format of A.B.C.D. metricvalue is the route metric. It must be an integer from 1 to 1024.
ip wins servers address
Configure WINS servers used by the WatchGuard device for services such as Mobile VPN and DHCP. address must be an IP address in the format of A.B.C.D. You can configure a maximum of three IP addresses. Use <u>no</u> ip wins servers to clear all WINS server addresses out of the configuration.

ip blocked-site dynamic <i>ip-address</i> expire-after day <i>dd</i> hour <i>hh</i> minute <i>min</i> second <i>sec</i>
Block all traffic from specified IP addresses for the specified time. <i>ip-address</i> is the host to be temporarily blocked. <i>dd</i> is the number of days from 0 to 365. <i>hh</i> is the number of hours from 0 to 23. <i>min</i> is the number of minutes from 0 to 59. <i>sec</i> is the number of seconds from 0 to 59.

Example:

```
ip allowed-site host 200.23.101.3
ip blocked-port 2000 log enable auto-blocked enable alarm blocked-ip-enable
enable launch-interval 60 repeat 3 action-type email
ip blocked-site www.example.com
ip blocked-site 200.23.103.0/24
ip blocked-site duration 15
ip dns domain-name watchguard.com
ip dns servers 192.168.1.1 192.168.1.2
ip dynamic-routing bgp
ip route 100.100.101.3 200
ip wins servers 192.168.1.1 192.168.1.2
```

log-setting

Description: Enable message logging facilities.

Syntax:

log-setting log-level <i>type level</i>
Control debug log messages of the type and level specified. <i>type</i> must be one of these options: <i>Authentication, FireCluster-2, Cluster-Management-3, Cluster-Operation-4, Cluster-Event-Monitoring-5, Cluster-Transport-6, Firewall-7, Management-8, Networking-9, DHCP-client-10, DHCP-server-11, PPP-12, PPPoE-13, Proxy-14, Connection-Framework-Manager-15, Session-Manager-16, DNS-17, FTP-18, H323-19, HTTP-20, HTTPS-21, POP3-22, SMTP-23, SIP-24, TCP-UDP-25, TFTP-26, Security-Subscriptions-27, Gateway-Antivirus-28, spamBlocker-29, WebBlocker-30, VPN-31, IKE-32, PPTP-33, SSLVPN-34, or Reputation-Authority-35.</i> <i>level</i> must be one of these options: <i>Off, Error, Warning, Information, or Debug.</i>
log-setting syslog-server enable <i>address option</i>
Send log messages to a remote syslog server. <i>address</i> is the IP address of a remote syslog server. It must be in the format of A.B.C.D. <i>option</i> must be one of these options: <i>default</i> or <i>type setting1 setting2.</i> <ul style="list-style-type: none"> - <i>type</i> must be one of these options: <i>alarm, event, traffic, debug, or support.</i> - <i>setting1</i> must be one of these options: <i>auth, priv-auth, cron, daemon, ftp, kern, lpr, mail, news, syslog, user, uucp, local0, local1, local2, local3, local4, local5, local6, or local7.</i> - <i>setting2</i> must be one of these options: <i>original, debug, info, notice, warning, err, crit, alert, or emerg.</i>
log-setting <i>type</i> enable
Enable the collection of a specified category of log messages. <i>type</i> must be one of these options: <i>ike-packet-trace, internal-storage, or performance-statistics.</i> Use no log-settings <i>type</i> to disable the category of log messages.
log-setting watchguard-log-server enable <i>ip-address key</i>
Specify the WatchGuard Log Server to which the device is to send log messages. <i>ip-address</i> is the IP address of the WatchGuard Log Server. <i>key</i> is the encryption key used to send information between the device and the Log Server.

Example:

```
log-setting log-level authentication debug
log-setting syslog-server 192.168.111.15 traffic ftp debug
log-setting ike-packet-trace enable
log-setting watchdog-log-server enable 10.0.1.50 s3cur!+y
```

managed-client

Description: Configure the device as a managed client.

Syntax:

managed-client device-name <i>name</i>
Add the name used to identify the managed client on the Management Server and in reports. <i>name</i> is a unique alphanumeric name that identifies the device.
managed-client enable
Enable the device as a managed client. No options available Use <u>no</u> managed-client to disable the administration of the device as a managed client.
managed-client certificate from <i>location</i>
Import a Management Server CA certificate. <i>location</i> must be either a valid FTP or TFTP address or the string <i>console</i> .
managed-client primary address password
Set primary Management Server. <i>address</i> is the IP address of the primary Management Server. It must be in the form of A.B.C.D. <i>password</i> is the unencrypted client shared secret.
managed-client secondary address password
Set one or more secondary Management Servers. <i>address</i> is the IP address of a secondary Management Server. It must be in the form of A.B.C.D. <i>password</i> is the unencrypted client shared secret. You can configure up to three secondary Management Servers.

Example:

```
managed-client certificate from tftp://myftpsite/files/upload/client.ca
managed-client enable
managed-client device-name FB001
managed-client primary 192.168.111.3 strongpass
managed-client secondary 192.168.140.4 strongpass 192.168.140.5 strongerpass
```

modem

Description: Configure modem settings for dial-up serial modem failover. For Firebox X Edge e-Series and XTM 2 Series devices only.

Syntax:

modem param enable
<p>Enable a modem parameter (param). Where param is one of these options:</p> <ul style="list-style-type: none"> <null> — Enable modem for dial-up failover when all external interfaces are down. manually-dns — Manually configure the DNS IP address. debug-trace — Enables the modem and Point-to-Point Protocol (PPP) debug trace. Use no modem param enable to disable the above modem commands options.
modem telephone tel-no name domain-name passwd dns1 dns2
<p>Configure the account settings of the dial-up failover.</p> <ul style="list-style-type: none"> tel-no is the remote access dial-in phone number of the Internet Service Provider. name is the user name for PPP authentication. domain-name is the domain name for PPP authentication. passwd is the password. dns1 is the primary DNS IP address. dns2 is the secondary DNS IP address.
modem account-name name domain-name passwd
<p>Configure or change the account settings of the dial-up failover modem; does not change the phone number.</p> <ul style="list-style-type: none"> name is the user name for PPP authentication. domain-name is the domain name for PPP authentication. passwd is the password.
modem alternate-telephone tel-no
<p>Add an alternate phone number for the dial-up modem.</p> <ul style="list-style-type: none"> tel-no is the remote access dial-in alternate phone number of the Internet Service Provider.
modem param value
<p>Configure modem options for the dial-up failover.</p> <p>param is one of these options:</p> <ul style="list-style-type: none"> dial-timeout is the dial-up timeout of the PPP negotiation if the modem does not connect. <ul style="list-style-type: none"> - value is time in seconds from 60 to 300; default is 120. redial-attempts is the number of dial-up attempts before it gives up the PPP negotiation. <ul style="list-style-type: none"> - value is number of redials from 0 to 5 default is 3. inactive-timeout is the inactive session timeout of the PPP connection. <ul style="list-style-type: none"> - value is time in minutes from 0 to 30; default is 0. mtu is Maximum Transmission Unit of the PPP connection. <ul style="list-style-type: none"> - value is in bytes is from 256 to 1500; default is 1500. primary-dns specifies the primary DNS in the DNS settings. <ul style="list-style-type: none"> - value is the IP address of the primary DNS. secondary-dns specifies the secondary DNS in the DNS settings. <ul style="list-style-type: none"> - value is the IP address of the secondary DNS. volume specifies the loudness of the modem's volume. <ul style="list-style-type: none"> - value must be one of these options: <i>Off, Low, Medium, or High</i>.
modem pppd-option option
<p>Configure ppp options.</p> <p>option is a ppp option that is required to make a connection. To specify more than one ppp option, separate the options with a comma and use double quotes around the list of options.</p>

<p>modem link-monitor ext-if lm-param option</p> <p>Define the Link Monitor configuration for Edge devices that use a dial-up backup. ext-if is the External Interface that is monitored to trigger a failover. lm-param is the Link Monitor parameter. lm-param must be one of these options together with its option.</p> <p>ping - Enable Ping to probe the remote side of the external link.</p> <ul style="list-style-type: none"> - option is host, the remote host to ping. This can be an IP address or a host name. - Use no modem link-monitor ext-if ping enable to disable ping probes. <p>tcp - Enable TCP to probe the remote side of the external link.</p> <ul style="list-style-type: none"> - option is host port where: host is the remote host to negotiate TCP session. This can be an IP address or a host name. The port is the port number to use for TCP negotiation, which is port 80 by default. If you do not specify a port number, the default value is used. - Use no modem link-monitor ext-if tcp enable to disable TCP probes. <p>both - A conditional state, which if enabled, requires the link monitor to satisfy both the ping and a TCP probe before the external interface is marked as active again.</p> <ul style="list-style-type: none"> - option is enable, both the ping and TCP probe are required for link monitoring. - Use no modem link-monitor ext-if both enable to require either ping or TCP probe only. <p>probe-interval - The time space between each link monitoring probe.</p> <ul style="list-style-type: none"> - option is sec, the time in seconds from 1 to 1200 and is 15 seconds by default. <p>deactivate-count - The number of consecutive link monitoring failures before it deactivates the external interface.</p> <ul style="list-style-type: none"> - option is number, the number of probes from 1 to 10 and is 3 by default. <p>reactivate-count - The number of consecutive link monitoring successes before it reactivates the external interface.</p> <ul style="list-style-type: none"> - option is number, the number of probes from 1 to 10; default is 3.

Example:

```
modem enable
modem account-name user1 domain.com mypa55w0rd 202.50.129.53 202.50.130.53
modem telephone 2061234 user1 example.com mypa55w0rd 202.50.129.53
202.50.129.54
modem alternate-telephone 2064321
modem dial-timeout 90
modem primary-dns 202.50.129.53
modem option receive-all
modem link-monitor 0 ping 196.24.1.1
modem pppd-option receive-all
```

multi-wan

Description: Configure the external interfaces to use multi-WAN features.

Syntax:

<p>multi-wan type interface</p> <p>Configure the selected interface to use a type of multi-WAN.</p> <p>type must be one of these options: <i>tcp-sticky-timer</i>, <i>udp-sticky-timer</i>, or <i>others-sticky-timer</i>.</p> <p>interface must be an integer from 0 to the maximum interface value on the device.</p>
<p>multi-wan failback-option option</p> <p>Set the action taken when the original address becomes available again.</p> <p>option must be one of these options: <i>gradual</i> or <i>immediate</i>.</p>

multi-wan load-balance failover <i>interface1 interface2</i>
<p>Set the failover sequence for interfaces in a multi-WAN failover configuration.</p> <p><i>interface1</i> is the name of the first interface to which traffic fails over.</p> <p><i>interface2</i> is the name of the second interface to which traffic fails over.</p> <p>You can enter as many interface names as you have interfaces configured for multi-WAN failover. There must be a minimum of two.</p>
multi-wan load-balance interface-overflow <i>interface1 threshold1 interface2 threshold2</i>
<p>Set the load balance overflow sequence in a multi-WAN interface overflow configuration.</p> <p><i>interface1</i> is the name of the first interface to which traffic is distributed.</p> <p><i>threshold1</i> is the threshold value in 100 Kbps increments. It must be an integer from 0 to 10000.</p> <p><i>interface2</i> is the name of the second interface to which traffic is distributed.</p> <p><i>threshold2</i> is the threshold value in 100 Kbps increments. It must be an integer from 0 to 10000.</p> <p>You can enter as many interface names as you have interfaces configured for multi-WAN interface overflow. There must be a minimum of two.</p>
multi-wan load-balance round-robin <i>interface1 weight1 interface2 weight2</i>
<p>Set the round-robin sequence in a multi-WAN round-robin configuration.</p> <p><i>interface1</i> is the name of the first interface to which traffic is distributed.</p> <p><i>weight1</i> is the round-robin weight. It must be an integer from 0 to 65535.</p> <p><i>interface2</i> is the identifying name of the second interface to which traffic is distributed.</p> <p><i>weight2</i> is the round-robin weight. It must be an integer from 0 to 65535.</p> <p>You can enter as many interface names as you have interfaces configured for multi-WAN round-robin. There must be a minimum of two.</p>
multi-wan load-balance routing-table <i>interface1 interface2</i>
<p>Set the interface sequence in a multi-WAN routing table configuration.</p> <p><i>interface1</i> is the name of the first interface to which traffic is distributed.</p> <p><i>interface2</i> is the name of the second interface to which traffic is distributed.</p> <p>You can enter as many interface names as you have interfaces configured for multi-WAN routing table. There must be a minimum of two.</p>
multi-wan link-monitor <i>interface interval frequency deactivate-count dcount reactivate-count rcount operation andor ping ICMPtarget TCP tcpaddress</i>
<p>Set the method to use to check the status of an interface configured for multi-WAN.</p> <p><i>interface</i> is the number of the external interface. It must be an integer from 0 to 7.</p> <p><i>frequency</i> is interval in seconds between probes. It must be an integer from 1 to 1200. The default value is 15.</p> <p><i>dcount</i> is the number of failures that must occur for the device to deactivate the interface. The default value is 3.</p> <p><i>rcount</i> is the number of successes that must occur for the device to reactivate the interface. The default value is 3.</p> <p><i>andor</i> sets whether the probe uses both TCP and PING to check the status, or only one. It must be either: <i>AND</i> or <i>OR</i>. The default value is <i>OR</i>.</p> <p><i>icmptarget</i> is the destination host that the device can ping to check the status. It must be either a domain name or an IP address in the format A.B.C.D.</p> <p><i>tcpaddress</i> is the IP address and port of a destination host, that the device can use to negotiate a TCP handshake to check status. It must be an address in the format A.B.C.D #, where # is an integer from 1 to 65535.</p>

Example:

```
multi-wan tcp-sticky-timer 0
multi-wan load-balance failover sequence 0 2 5 6
multi-wan load-balance round-robin weights 0 10
multi-wan 2 interval 30 deactivate-count 5 reactivate-count 2 operation and
icmp 192.168.32.2 tcp 192.168.33.2 28
```

network-mode

Description: Set the network mode.

If you use bridge mode, your Firebox or XTM device cannot complete some functions that require it to operate as a gateway. These functions include: multi-WAN, VLANs, network bridges, static routes, FireCluster, secondary networks, DHCP server or DHCP relay, serial modem failover, NAT, dynamic routing, any type of VPN for which the Firebox is an endpoint or gateway, and some proxy functions, including HTTP Web Cache Server.

Syntax:

<p>network-mode option</p> <p>Set the network mode to Routed, Drop-in or Bridge mode.</p> <p>option must be one of these options: <i>routed</i>, drop-in <i>address gateway</i>, or bridge <i>address gateway</i>.</p> <ul style="list-style-type: none"> - <i>address</i> is the IP address used as the primary address for all interfaces on the device. It is either an address with netmask in the format of A.B.C.D A.B.C.D. or a network in the format of A.B.C.D/#, where # must be in the range of 8 to 30. - <i>gateway</i> is the IP address of default gateway. It must be in the form A.B.C.D.
<p>network-mode auto-host-mapping if-number setting if-number setting</p> <p>Specify the interface for automatic host mapping.</p> <p>if-number is the interface index number.</p> <p>setting must be one of these options: <i>enable</i> or <i>disable</i>.</p> <p>You can specify more than one interface with their respective settings.</p>
<p>network-mode dhcp relay serverip</p> <p>Configure to relay DHCP requests to the specified server.</p> <p>serverip is the IP address of the DHCP server that is used for computers on the interface.</p> <p>Use no dhcp enable to disable DHCP relay on the interface.</p>
<p>network-mode dhcp server start-addr startip endip leasetime dns-server dns* domain domainname reservation resvname macaddress ipaddress wins wins*</p> <p>Configure as a DHCP server for computers connected to the device.</p> <p>start-addr defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with these parameters:</p> <ul style="list-style-type: none"> - startip is the first IP address in the DHCP address pool. - endip is the last IP address in the DHSCP address pool. <p>leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer.</p> <p>dns* is the IP address of one or more valid DNS servers.</p> <p>domainname is the domain name used by devices on the network.</p> <p>reservation defines a pair of MAC address and IP address that are reserved within the DHCP address pool. In the same line, you can use the reservation command multiple times with these parameters:</p> <ul style="list-style-type: none"> - resvname is a string to identify a reserved address. - macaddress is the MAC address of the device with a reserved address. - ipaddress is the IP address assigned to the reserved address. <p>Use no dhcp enable to disable DHCP server on the interface.</p>
<p>network-mode related-host ip-address if-number</p> <p>ip-address is the IP address that is related to the interface.</p> <p>if-number is the interface index that is related to the IP address.</p>

Example:

```
network-mode routed
network-mode drop-in 200.100.100.0/24 200.200.200.3
network-mode auto-host-mapping 3 enable 4
```

ntp

Description: Configure the device to get timestamps from an NTP server.

Syntax:

ntp enable
No options available. Use <u>no</u> ntp to disable use of an NTP server.
ntp server ip address
Add an NTP server with an IP address. address is the IP address of an NTP server in the format A.B.C.D. Use <u>no</u> ntp server ip address to remove an NTP server from the configuration.
ntp server domain hostname
Add an NTP server with a domain name. hostname is the hostname (FQDN) of an NTP server. Use <u>no</u> ntp server domain hostname to remove an NTP server from the configuration.

Example:

```
ntp server ip 200.220.100.12
ntp server domain ntp.foo.org
no ntp server ip 203.201.39.1
```

policy

Description: Enter the Policy command mode.

Syntax:

policy
No options available.

Example:

```
interface policy
WG(config/policy)#
```

signature-update

Description: Configure a device to get updated signature files for IPS and Gateway Antivirus.

Syntax:

signature-update component action
Enable or disable automatic updates for the specified component. component must be one of these options: <i>IPS</i> or <i>GAV</i> . action must be either: <i>enable</i> , or <i>disable</i> .
signature-update interval
Configure the Gateway AV and IPS update interval interval is the frequency between updates, measured in hours.
signature-update server-url https-url
Configure the secure URL of the update server. url is the URL of the update server. It must be in the format: <i>https://host/url-path</i> .
signature-update update component
Trigger an immediate signature update for the specified component. component must be one of these options: <i>IPS</i> or <i>GAV</i> .

Example:

```
signature-update gav enable
signature-update update gav
```

snmp

Description: Configure the device to integrate with SNMP tools.

Syntax:

snmp servers address
Configure SNMP management computers. address is an IP address in the format A.B.C.D. You can configure up to three SNMP management computers. Use no snmp server address to remove an SNMP management computer from the configuration.
snmp version v1_2 community string
Configure the device to use SNMP version 1 or 2 polling. string is the value of the community string.
snmp snmp-version v3 username authprotocol authpassword privacytype
Configure the device to use SNMP version 3 polling. username is a string for the SNMP user name. authprotocol is the authentication protocol. It must be one of these options: <i>MD5</i> or <i>SHA1</i> authpassword is the user password on the SNMP management computer. privacytype is the privacy protocol. It must be either: DES <i>despassword</i> or <i>None</i> . - <i>despassword</i> is the password used to encrypt DES on the SNMP management computer.
snmp traps enable type
Enable SNMP traps for the device. type must be one of these options: <i>trap v1</i> , <i>trap v2c</i> , <i>trap v3</i> , <i>inform v2</i> , or <i>inform v3</i> .

Example:

```
snmp servers 100.100.2.4 100.100.3.3
snmp version v3 watchguard MD5 strongpass des str0ngpa55.
snmp traps enable inform v3
```

static-arp

Description: Create an IP address to MAC address binding.

Syntax:

static-arp name ip-address mac-address
<i>name</i> is the name of the interface.
<i>ip-address</i> is the IP address of the computer.
<i>mac-address</i> is the physical address of the computer.

Example:

```
static-arp user1 10.0.1.56 00:1F:3C:C7:70:9A
```

system

Description: Set global device properties.

Syntax:

system contact string
<i>string</i> is the name of the system administrator.
system location string
<i>string</i> is the geographic location of the device.
system name string
<i>string</i> is the friendly name of the device as it appears in reports and graphic displays.
system timezone zone
<i>zone</i> is the timezone of the device. It must be a two digit integer from 00 to 62. To get a list of <i>zone</i> values, type help system timezone ?

Example:

```
system contact Joe Parchese
system name BigCoHeadquarters
system location Seattle
system timezone 04
```

vlan

Description: Create or edit a VLAN virtual interface on the device.

Syntax:

vlan <i>vlanname</i>
<i>vlanname</i> is a string that uniquely identifies the VLAN. Use <u>no</u> vlan <i>vlanname</i> to delete the VLAN virtual interface.

After you enter the command **vlan *vlanname***, the configuration continues to the VLAN details command. The prompt changes to “wg(config/vlan-*vlanname*)#”. Use the **Exit** command to exit this mode.

vlan-id <i>id</i> security-zone <i>zone</i> address member <i>if-number</i> <i>option</i> <i>if-number</i> <i>option</i>
<i>id</i> is the VLAN unique identifier numbers from 1 to 4094. <i>zone</i> is the security zone. It must be one of these options: external, trusted, or optional. <i>address</i> is the IP address assigned to the virtual interface. <ul style="list-style-type: none"> - For Trusted and Optional Zones it is either an address with mask in the format of A.B.C.D A.B.C.D. or a net in the format of A.B.C.D/# where # must be in the range of 8 to 30. - For the External Zone it can be one of these options: <i>static-ip</i>, <i>dhcp</i> or <i>pppoe</i>. <i>if-number</i> is the interface index that is assigned as a member of the VLAN. <i>option</i> must be one of these options: <i>tagged</i> , or <i>untagged</i> . You can specify more than one member interface of the VLAN.

Example:

```
vlan VLAN10
vlan-id 10 security-zone trusted 10.10.1.1/24 member 3 tagged 4 tagged
```

vpn-setting

Description: Enable global VPN settings.

Syntax:

vpn-setting <i>setting</i> enable
<i>setting</i> must be one of these settings: <ul style="list-style-type: none"> - <i>ldap</i> — enable the use of an LDAP server for certificate verification. - <i>pass-through</i> — enable IPSec pass-through. - <i>security-readonly</i> — make the security policy read-only in the Mobile VPN with IPSec client. - <i>tos-tunnel-flag</i> — enable TOS (Type of Service) for IPSec. Use <u>no</u> vpn-setting <i>setting</i> enable to disable a global VPN setting.
vpn-setting ldap server <i>server</i> <i>port</i>
Set the LDAP server to use for certificate verification. <ul style="list-style-type: none"> - <i>server</i> is the IP address of the LDAP server, in the format A.B.C.D. - <i>port</i> is the port number to use on the LDAP server.
vpn-setting notification notification enable <i>action-type</i> <i>action-type</i> launch-interval <i>launch-interval</i> repeat-count <i>repeat-count</i>
Configure VPN notification settings. <i>action-type</i> must be one of these settings: <ul style="list-style-type: none"> - <i>email</i> — the Log Server sends an email to the configured email address when the event occurs. - <i>pop-window</i> — the Log Server opens a dialog box when the event occurs. <i>launch-interval</i> is the minimum time (in minutes) between different notifications, default is 15. <i>repeat-count</i> is the number of events to include in a repeat log notification, default is 10.

vpn-setting notification snmp-trap enable
Enable the device to send an event notifications to the configured SNMP management system.
vpn-setting ipsec-pkt-error-log <i>loglevel</i>
Enable or disable IPsec log message error types. <i>loglevel</i> must be one of these settings: <ul style="list-style-type: none"> - 0 — disable all IPsec error log messages - 1 — enable Invalid SPI log messages - 2 — enable Replay Window Check failure log messages - 4 — enable Replay Check failure log messages - 8 — enable AH integrity check failure log messages - 16 — enable ESP integrity check failure log messages - 31 — enable all IPsec error logs

Example:

```
vpn-setting pass-through
vpn-setting tos-tunnel-flag
vpn-setting ldap enable
vpn-setting ldap server 100.100.100.50 389
vpn-setting notification notification enable action-type email
vpn-setting notification snmp-trap enable
vpn-setting ipsec-pkt-error-log 2
vpn-setting ipsec-pkt-error-log 0
```

web-server-cert

Description: Configure the web server certificate to use for authentication to Fireware XTM Web UI.

Syntax:

web-server-cert custom <i>common-name org-name org-unit-name dns dns-ip ip extended-ip</i>
Use a custom certificate signed by your WatchGuard device. The certificate automatically includes all trusted interface IP addresses. <i>common-name</i> is a string for the common name of your organization. This is usually the domain name. <i>org-name</i> is a string for the organization name. <i>org-unit-name</i> is a string for the organizational unit name. <i>dns-ip</i> is a string for an additional IP address to include in the certificate. <i>extended-ip</i> is a string for an additional domain name to include in the certificate.
web-server-cert default
Use the default certificate.
web-server-cert third-party certificate-id
Use a certificate you have imported previously. <i>certificate-id</i> is the certificate identification number, between 0 and 99999.

Example:

```
web-server-cert default
web-server-cert third-party 1234
web-server-cert custom example.com exampleco hq
```

wireless

Description: Configure Wi-Fi settings for Firebox X Edge e-Series and XTM 2 Series wireless devices.

Syntax:

wireless client enable
Enable wireless client as an external interface. Use no wireless client enable to disable this setting.
wireless client dhcp-client <i>client clientname host-name hostname l-time ip-address</i>
Configure wireless client settings when negotiating with a DHCP server. <i>clientname</i> is a string for the optional client name. <i>hostname</i> is a string for the optional hostname. <i>l-time</i> is a string for the optional lease time from 1 to 2147483647. <i>ip-address</i> is a string for the optional preferred IP address. any use this option instead of <i>ip-address</i> to enable DHCP to assign an IP address automatically.
wireless client manual-conf <i>ip-address mask gateway</i>
Manually configure the wireless client IP address. <i>ip-address</i> is the wireless client IP address. <i>mask</i> is the subnet mask in dotted decimal notation. <i>gateway</i> is the default gateway of the wireless external interface.
wireless <i>apname wireless ssid auth enc enc-option</i>
Configure wireless authentication and encryption settings. <i>apname</i> is the Wi-Fi option. It must be one of these options: <i>client, access-point1, access-point2</i> or <i>guest</i> . <i>ssid</i> is a string for the network name. <i>auth</i> is the authentication options. It must be one of these options: <i>open-system, shared-key, wpa-only, wpa-wpa2, wpa2-only</i> . <i>enc</i> is the encryption option. The encryption option is dependent on the authentication option you select, and is based on these options: <ul style="list-style-type: none"> - for <i>open-system</i>, enc must be one of these options: <i>disable, wep-128-ascii, wep-128-hex, wep-40-ascii, wep-64-hex</i>. - for <i>shared-key</i>, enc must be one of these options: <i>wep-128-ascii, wep-128-hex, wep-40-ascii, wep-64-hex</i>. - for <i>wpa-only, wpa-wpa2</i> and <i>wpa2-only</i>, enc must be one of these options: <i>aes, auto</i> or <i>tkip</i>. You cannot use <i>tkip</i> as the encryption method if you use a wireless mode that supports 802.11n. enc-option is the option needed to complete the encapsulation. This dependent on the encryption option you select and is as follows: <ul style="list-style-type: none"> - for <i>disable</i>, enc-option is Null. - for <i>wep-128-ascii, wep-128-hex, wep-40-ascii, and wep-64-hex</i>, enc-option must be a combination of <i>key-index</i>, which is an integer from 1 to 4, and <i>key</i>, length and type of which is defined on the selected encapsulation. - for <i>aes, auto</i> and <i>tkip</i>, enc-option is the passphrase.

wireless guest hotspot enable
Enable the hotspot on the wireless guest network. Use no wireless guest hotspot enable to disable the hotspot.
wireless guest hotspot timeout-type <i>day days hour hours minute minutes second seconds</i>
Configure the timeout settings for wireless hotspot connections. timeout-type is the hotspot timeout option. It must be one of these options: <i>session-timeout</i> , or <i>idle-timeout</i> . <i>days</i> is the duration in days. It must be an integer from 0 to 365. <i>hours</i> is the duration in hours. It must be an integer from 0 to 23. <i>minutes</i> is the duration in minutes. It must be an integer from 0 to 59. <i>seconds</i> is the duration in seconds. It must be an integer from 0 to 59. If session-timeout is set to 0 (the default value), user sessions never time out based on total time connected. If idle timeout is set to 0, user sessions never time out based on inactivity. The default idle timeout is 2 hours.
wireless guest hotspot title "<i>title-text</i>"
Configure the text that appears as the title on the wireless hotspot splash screen. title-text is the title for the splash screen. It must be enclosed in double quotes.
wireless guest hotspot welcome-message input "<i>message-text</i>"
Configure the welcome message that appears below the title on the wireless hotspot splash screen. message-text is the welcome message. It must be enclosed in double quotes. The maximum length is 2,000 characters.
wireless guest hotspot welcome-message from <i>location</i>
Import the welcome message for the wireless hotspot from a text file. location must be either an FTP or TFTP address.
wireless guest hotspot terms-text input "<i>terms-text</i>"
Configure the terms and conditions text that appears on the wireless hotspot splash screen. terms-text is the terms and conditions text. It must be enclosed in double quotes. The maximum length is 20,000 characters.
wireless guest hotspot terms-text from <i>location</i>
Import the terms and conditions text for the wireless hotspot from a text file. location must be either an FTP or TFTP address.
wireless guest hotspot import logo from <i>location</i>
Import a custom logo file to use on the hotspot splash screen. location must be either an FTP or TFTP address.
wireless guest hotspot use-logo <i>option</i>
Choose whether to use a custom logo or the default logo. option must be one of these settings: <i>custom</i> or <i>default</i> .
wireless guest hotspot auto-redirect <i>url-path</i>
Redirect the browser to a specified web site after the user accepts the terms and conditions. url-path is the web site to automatically redirect the browser to.

<p>wireless guest hotspot font-name <i>font</i> font-size <i>font-size</i> font-color "<i>text-color</i>" background-color "<i>background-color</i>"</p> <p>Customize the font and color settings for the hotspot splash screen. You can specify only one of these settings on the command line at a time.</p> <p><i>font</i> must be one of these values: <i>arial</i>, <i>comic-sans-ms</i>, <i>courier-new</i>, <i>georgia</i>, <i>lucida-console</i>, <i>microsoft-sans-serif</i>, <i>tahoma</i>, <i>times-new-roman</i>, <i>trebuchet-ms</i>, <i>verdana</i>.</p> <p><i>font-size</i> must be one of these values: <i>xx-small</i>, <i>small</i>, <i>medium</i>, <i>large</i>, <i>x-large</i>, <i>xx-large</i>.</p> <p><i>text-color</i> must be a hex color code, default is #000000 (black).</p> <p><i>background-color</i> must be a hex color code, default is #FFFFFF (white).</p> <p>Specify the hex color code for <i>text-color</i> and <i>background-color</i>, in the format "#RRGGBB" where RR is Red, GG is Green, and BB is Blue. Each character must be a hex value <[-](alpha 0-9)(alpha 0-9 _ .)*>. You must use quotes around these color codes.</p>
<p>no wireless guest hotspot users <i>param</i> <i>address</i></p> <p>Disconnect one or all wireless clients from your wireless guest hotspot.</p> <p><i>param</i> must be one of these values:</p> <ul style="list-style-type: none"> - <i>all</i> — Disconnect all connected wireless clients from the hotspot. - <i>ip</i> — Disconnect the wireless client with the IP address specified in the <i>address</i> parameter. - <i>mac</i> — Disconnect the wireless client with the MAC address specified in the <i>address</i> parameter. <p>Use the show wireless guest hotspot users command to see a list of connected wireless clients.</p>
<p>wireless apname enable</p> <p>Enable the access point.</p> <p><i>apname</i> must be one of these options: <i>access-point1</i>, <i>access-point2</i>, or <i>guest</i>.</p> <p>Use no wireless apname enable to disable the access point.</p>
<p>wireless apname broadcast enable</p> <p>Enable SSID broadcasts for the specified access point.</p> <p><i>apname</i> must be one of these options: <i>access-point1</i>, <i>access-point2</i>, or <i>guest</i>.</p> <p>Use no wireless apname broadcast enable to disable SSID broadcasts for this access point.</p>
<p>wireless apname interface zone</p> <p>Select whether to bridge the wireless network to the Trusted or Optional interface.</p> <p><i>apname</i> must be one of these options: <i>access-point1</i>, <i>access-point2</i>, or <i>guest</i>.</p> <p><i>zone</i> must be either <i>trusted</i> or <i>optional</i>.</p>
<p>wireless apname log-auth enable</p> <p>Enable authentication event logging for the specified access point.</p> <p><i>apname</i> must be one of these options: <i>access-point1</i>, <i>access-point2</i>, or <i>guest</i>.</p> <p>Use no wireless apname log-auth enable to disable authentication event logging for this access point.</p>
<p>wireless apname mac-acl enable</p> <p>Enable MAC access control for the specified access point.</p> <p><i>apname</i> must be one of these options: <i>access-point1</i>, <i>access-point2</i>, or <i>guest</i>.</p> <p>Use no wireless apname broadcast enable to disable MAC access control for this access point.</p>
<p>wireless apname mac-acl mac-address</p> <p>Add a MAC address to the list of allowed address for MAC access control.</p> <p><i>apname</i> must be one of these options: <i>access-point1</i>, <i>access-point2</i>, or <i>guest</i>.</p> <p><i>mac-address</i> is the MAC address of a computer you want to give access to this access point.</p>
<p>wireless apname requirevpn enable</p> <p>Require encrypted Mobile VPN with IPSec connections to the specified access point.</p> <p><i>apname</i> must be one of these options: <i>access-point1</i>, <i>access-point2</i>, or <i>guest</i>.</p> <p>Use no wireless apname requirevpn enable to not require encrypted Mobile VPN with IPSec connections to this access point.</p>

wireless <i>apname</i> frag-threshold <i>threshold</i>
Change the fragmentation threshold for the specified access point. <i>apname</i> must be one of these options: <i>access-point1</i> , <i>access-point2</i> , or <i>guest</i> . <i>threshold</i> is the fragmentation threshold, in bytes. It must be an integer from 256 to 2346.
wireless <i>apname</i> rts-threshold <i>threshold</i>
Change the request to send threshold for the specified access point. <i>apname</i> must be one of these options: <i>access-point1</i> , <i>access-point2</i> , or <i>guest</i> . <i>threshold</i> is the request to send threshold, in bytes. It must be an integer from 256 to 2346.
wireless radio-settings <i>band mode channel</i>
Configure wireless radio settings for a WatchGuard XTM 2 Series wireless device. The available values for <i>band</i> , <i>mode</i> and <i>channel</i> are different for each wireless region. <i>band</i> is the wireless band. It must be one of these values: <ul style="list-style-type: none"> - 24 — 2.4 Ghz - 5 — 5 Ghz <i>mode</i> is the wireless mode. It must be one of these values: <ul style="list-style-type: none"> - IEEE80211bg — 802.11b and 802.11g (2.4 Ghz band only) - IEEE802.11bonly — 802.11b only (2.4 Ghz band only) - IEEE80211nbg — 801.11n, 802.11b, and 802.11g (2.4 Ghz band only) - IEEE80211an — 80211a and 802.11n (5 Ghz band only) - IEEE80211aonly — 802.11a only (5 Ghz band only) <i>channel</i> is the wireless channel. <ul style="list-style-type: none"> - For the 2.4 GHz band, <i>channel</i> must be one of these values: <i>auto</i>, <i>channel-01</i>, <i>channel-02</i>, <i>channel-03</i>, <i>channel-04</i>, <i>channel-05</i>, <i>channel-06</i>, <i>channel-07</i>, <i>channel-08</i>, <i>channel-09</i>, <i>channel-10</i>, <i>channel-11</i>, <i>channel-12</i>, <i>channel-13</i>, or <i>channel-14</i>. - For the 5 GHz band, <i>channel</i> must be one of these values: <i>auto</i>, <i>channel-36</i>, <i>channel-40</i>, <i>channel-44</i>, <i>channel-48</i>, <i>channel-149</i>, <i>channel-153</i>, <i>channel-157</i>, <i>channel-161</i>, or <i>channel-165</i>. The available channels depend on the country where the device is operating and the wireless mode you select. - When you set <i>channel</i> to <i>auto</i>, the 2-Series wireless device automatically selects a quiet channel from the available channels in the selected band.
wireless radio-settings <i>option</i>
Configure wireless radio settings for a Firebox X Edge e-Series wireless device. <i>option</i> must be one of these options: <ul style="list-style-type: none"> - <i>channel</i> is the channel from 0 to 14; 0 is auto. - <i>mode</i> is the radio mode either <i>IEEE-802dot11g</i>, <i>IEEE-802dot11b</i>, or <i>both</i>. - <i>region op-region</i> is the operating region. It must be one of these values: <i>Australia</i>, <i>PRC</i>, <i>Taiwan</i>, <i>France</i>, <i>EMEA</i>, <i>Israel</i>, <i>Asia</i>, or <i>Americas</i>.

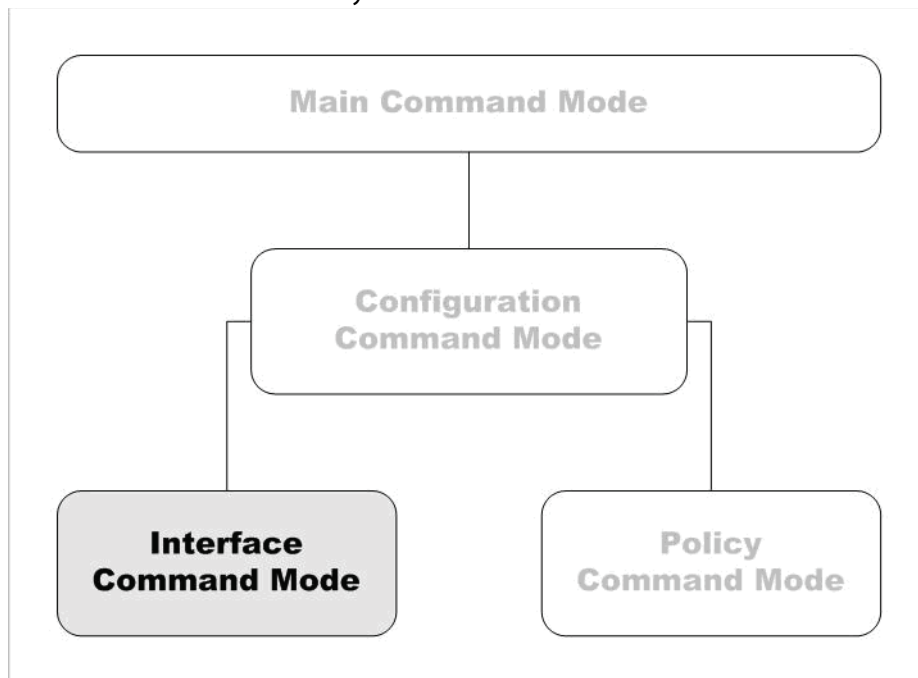
Example:

```
wireless client enable
wireless client dhcp-client 100.100.100.10 172800
wireless client manual-conf 100.100.100.10 255.255.255.0 100.100.100.1
wireless access-point1 enable
wireless access-point1 wireless AP01 shared-key wep-64-hex 1 ab00ab00ab
wireless access-point1 broadcast enable
wireless guest enable
wireless guest wireless guestAP01 shared-key wep-64-hex 1 ab00ab00ab
wireless guest hotspot title "WatchGuard hotspot"
wireless guest hotspot terms-text from tftp://myserver/terms.txt
wireless guest hotspot import logo from tftp://myserver/customlogo.jpg
wireless guest hotspot use-logo custom
wireless radio-settings region Americas
wireless radio-settings both
```


6

Interface Command Mode

The WatchGuard Command Line Interface (CLI) Interface command mode is used to configure the separate Ethernet interfaces available on your Firebox or XTM device.



In the Interface mode, you can:

- Configure the IP address and addressing options for the interface
- Configure the interface as a gateway
- Control MTU and link speed preferences
- Configure the interface as a DHCP server or DHCP relay
- Configure the interface for QoS

Enter the Interface Command Mode

To enter the Interface command mode:

- 1 Open the CLI in the Configuration command mode.
- 2 Type the **interface fastethernet <if-index>** command, where **<if-index>** is the interface number, from 0 to the number of interfaces minus 1.
- 3 Press **Enter**.
In Interface command mode, the CLI prompt changes to WG(config/if-fe<if-index>)# where <if-index> is the selected interface.

You can only configure a single Ethernet interface at a time. To configure another interface, exit the Interface mode. From the Configuration mode, use the **interface** command again to select the second interface.

List of Interface Mode Commands

You can use all common commands in the Interface command mode. For more information, see “List of Common Commands” on page 15.

These commands are available only in Interface mode:

Command	Usage
dhcp	Enable the interface as either a DHCP server or relay.
enable	Enable or disable the physical interface.
ip	Configure the IP address and addressing options for the interface.
link-speed	Set the link speed and duplex for the interface.
mac-access-control	Configure a trusted or optional interface to restrict access based on MAC address.
mac-ip-binding	Bind the Ethernet MAC address to a particular IP address.
mtu	Control the interface MTU settings.
name	Set the name for the interface as it appears in reports and the user interface.
pppoe	Configure the Point-to-Point over Ethernet Protocol for the external interface.
qos	Enable QoS Marking for traffic that goes out of the interface.
secondary	Configure the secondary IP addresses that the interface uses to route traffic.
type	Set the interface type.
vpn-pmtu	Configure the Per Interface Maximum Transmission Unit for external interface only.

Interface Command Mode Reference

dhcp

Description: Enable the interface as either a DHCP server or relay. Or, enable the external interface as a DHCP client to dynamically get an IP address from an external DHCP server.

Syntax:

dhcp relay serverip
Configure a trusted or optional interface to relay DHCP requests to the specified server. serverip is the IP address of the DHCP server that is used for computers on the interface. Use no dhcp enable to disable DHCP relay on the interface.
dhcp server start-addr startip endip leasetime dns-server dns* domain domainname reservation resvname macaddress ipaddress wins wins*
Configure the trusted or optional interface as a DHCP server for computers on that interface. start-addr defines a DHCP address pool. In the same line, you can use the start-addr command multiple times with these parameters: <ul style="list-style-type: none"> - startip is the first IP address in the DHCP address pool. - endip is the last IP address in the DHCP address pool. leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer. dns* is the IP address of one or more valid DNS servers. domainname is the domain name used by devices on the network. reservation defines a pair of MAC address and IP address that are reserved within the DHCP address pool. In the same line, you can use the reservation command multiple times with these parameters: <ul style="list-style-type: none"> - resvname is a string to identify a reserved address. - macaddress is the MAC address of the device with a reserved address. - ipaddress is the IP address assigned to the reserved address. Use no dhcp enable to disable DHCP server on the interface.
dhcp any leasetime
Configure the external interface to get a DHCP-assigned IP address from the ISP. leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer. Use no dhcp to disable DHCP client on the interface.
dhcp host-id hostid host-name hostname ipaddress leasetime
Configure a detailed DHCP client on the External interface. hostid is the Host ID to use to negotiate an IP address from the DHCP server. hostname is the Host Name to use to negotiate an IP address from the DHCP server. ipaddress is to force the DHCP server to lease a specific IP address. leasetime is the duration in hours that addresses are leased to devices on the network. The value must be an integer. Use no dhcp host-name host-id lease-time to disable detailed DHCP client on the interface.

Example:

```
dhcp relay 10.0.1.254
dhcp server start-addr 10.0.1.2 10.0.1.30 8
dhcp server start-addr 10.0.1.2 10.0.1.30 8 dns-server 203.23.124.1
203.23.124.2 domain watchguard.com reservation ceo 00:44:FF:33:00:AC
10.0.1.35 wins 10.0.1.100
dhcp server wins 10.0.1.100
```

enable

Description: Enable or disable the physical interface.

Syntax:

enable
No options available. Use <u>no</u> enable to disable the interface.

ip

Description: Configure the IP address and addressing options for the interface.

Syntax:

ip address option
Set the IP address of an interface. option must be one of these options: <i>addr mask</i> or <i>net</i> <ul style="list-style-type: none"> - <i>addr</i> is an IP address, and must be in the format of A.B.C.D. - <i>mask</i> is an IP subnet mask, and must be in the format of A.B.C.D. <i>net</i> is the IP address and subnet prefix in the format of A.B.C.D/#, where # must be in the range of 0 to 32.
ip df flag
Configure Don't Fragment bit on the external interface. <ul style="list-style-type: none"> - flag must be one of these options: <i>clear</i>, <i>set</i>, or <i>copy</i>.

Example:

```
ip address 192.168.116.1 255.255.255.0
ip address 192.168.116.1/24
ip df set
```

link-speed

Description: Set the interface link speed and duplex.

Syntax:

link-speed option
option must be one of these options: <ul style="list-style-type: none"> - <i>10-full</i> — Force 10 Mbps full-duplex operation - <i>10-half</i> — Force 10 Mbps half-duplex operation - <i>100-full</i> — Force 100 Mbps full-duplex operation - <i>100-half</i> — Force 100 Mbps half-duplex operation - <i>1000-full</i> — Force 1000 Mbps full-duplex operation (available only if the interface supports it) - <i>1000-half</i> — Force 1000 Mbps half-duplex operation (available only if the interface supports it) For a description of which interfaces support a link speed of 1000 Mbps, see the Hardware Guide for your device.

Example:

```
link-speed 100-full
```

mac-access-control

Description: Control access to the trusted or optional interface of a WatchGuard device by computer MAC address.

Syntax:

mac-access-control enable *mac-address*

Enable MAC access control on an interface, or add a MAC address to the allowed list.

mac-address is the MAC address of a computer that is allowed to send traffic on this interface. The MAC address must be in the format of 00:01:23:45:67:89.

Use **no mac-access control enable *mac-address*** to remove a MAC address of a computer from the list of MAC addresses that are allowed to send traffic on this interface.

Use **no mac-access control enable** to disable MAC access control on the interface.

Example:

```
mac-access-control enable
mac-access-control 00:01:23:45:67:89
```

mac-ip-binding

Description: Control access to a WatchGuard device interface from an IP address by computer hardware address.

Syntax:

mac-ip-binding *ipaddress macaddr*

Use to add MAC addresses to a network interface.

ipaddress is the IP address of the interface.

macaddr is one or more hardware device addresses that can connect to the interface.

This command can have more than one IP address to MAC address pairs.

Use **no mac-ip-binding *ipaddress macaddr*** to disable MAC address binding on this interface.

mac-ip-binding restrict-traffic enable

Use to restrict traffic based on the IP address and MAC addresses already configured for the interface.

Use **no mac-ip-binding restrict-traffic enable** to disable binding traffic restrictions on this interface.

Example:

```
mac-ip-binding 100.100.100.3 00:44:FF:33:00:AC 00:44:FF:33:00:F0
mac-ip-binding restrict-traffic enable
```

mtu

Description: Set the Maximum Transmission Unit value of an interface.

Syntax:

mtu *size*

size is the size in bytes of the maximum transmission unit. Must be an integer from 68 to 9000.

Example:

```
mtu 1024
```

name

Description: Set the interface name or alias as it appears in log messages and user interfaces.

Syntax:

name string
<i>string</i> is the new name of the interface.

Example:

```
name publicservers
```

pppoe

Description: Configure the external interface to negotiate PPPoE with the ISP.

Syntax:

pppoe auth reauth ac-name acname auth-timeout timeout service-name serv
Configure PPPoE authentication settings. <i>reauth</i> is the allowed number of authentication retries from 0 to 20. <i>acname</i> is the Access Concentrator Name. <i>timeout</i> is the number of seconds between each connection attempt from 0 to 60. <i>serv</i> is the PPPoE Service Name. Use <u>no</u> pppoe auth with any of the previous parameters to disable the setting.
pppoe auto-reboot enable day hour minute
Configure a scheduled automatic restart of the PPPoE session. <i>day</i> is the day of the week to restart. It must be one of these options: - 0 — Sunday - 1 — Monday - 2 — Tuesday - 3 — Wednesday - 4 — Thursday - 5 — Friday - 6 — Saturday - 7 — Daily <i>hour</i> is the hour of the day to restart. It must be an integer from 0 to 23. <i>minute</i> is the minute of the hour to restart. It must be an integer from 0 to 59. Use <u>no</u> pppoe auto-reboot enable to disable automatic restart.
pppoe connection type time
Configure PPPoE connection settings. <i>type</i> must be either: <i>always-on</i> or <i>dial-on-demand</i> . <i>time</i> must be either: - if <i>type</i> is <i>always-on</i> , <i>time</i> is the auto-reconnect time in seconds from 0 to 3600. - if <i>type</i> is <i>dial-on-demand</i> , <i>time</i> is the inactivity timeout in minutes from 0 to 60.
pppoe host-uniq enable
Enable the host-uniq tag in PPPoE discovery packets. Use <u>no</u> pppoe host-uniq enable to disable the host-uniq tag.
pppoe lcp-echo enable retries lcp-timeout lcp-timeout
Configure the use of LCP echo requests to detect lost PPPoE connections. <i>retries</i> is the number of LCP retries in seconds from 1 to 60. <i>lcp-timeout</i> is the LCP echo timeout in seconds from 1 to 1200. Use <u>no</u> pppoe lcp-echo enable to disable LCP echo requests.

pppoe static-ip <i>ipaddress</i>
Configure a static IP address. <i>ipaddress</i> force PPPoE to use this static IP address. Use no pppoe static-ip to remove the static IP address and get an IP address automatically.
pppoe user-info <i>username password</i>
Configure the user login information. <i>username</i> is the string PPPoE user name. <i>password</i> is the PPPoE password.

Example:

```
pppoe user-info myuser mypasswd
pppoe static-ip 100.100.100.10
pppoe connection always-on 30
pppoe auth 3 ac-name concentrator1 auth-timeout 10
pppoe auth service-name serviceA
pppoe connection dial-on-demand 60
no pppoe auth ac-name
pppoe auto-reboot enable day 3
pppoe auto-reboot enable hour 2
pppoe lcp-echo enable 3 lcp-timeout 30
```

qos

Description: Configure Quality of Service settings for the interface.

Syntax:

qos marking dscp <i>state priority-method method</i>
<i>state</i> is the DSCP state and must be one of these values: <i>assign type, clear, or preserve</i> . <ul style="list-style-type: none"> - If <i>state</i> is <i>assign</i>, you must add a string for <i>type</i>. - <i>type</i> is the DSCP assign method and must be one of these values: <i>Best-effort, CS1-Scavenger, AF11, AF12, AF13, CS2, AF21, AF22, AF23, CS3, AF31, AF32, AF33, CS4, AF41, AF42, AF43, CS5, EF, Control-CS6, or Control-CS7</i>. <i>method</i> is the method used to assign priority and must be one of these values: <i>No_Priority, Customer, or Mapped-from-Marking</i> .
qos marking precedence <i>state priority-method method</i>
<i>state</i> is the precedence state and must be one of these values: <i>assign value, clear, or preserve</i> . <ul style="list-style-type: none"> - If <i>state</i> is <i>assign</i>, you must add a string for <i>value</i>. - <i>value</i> is the precedence value. It must be an integer from 0 to 7. <i>method</i> is the method used to assign priority and must be one of these values: <i>No_Priority, Customer, or Mapped-from-Marking</i> .
qos max-link-bandwidth <i>value</i>
<i>value</i> is the maximum link bandwidth in bytes. It must be an integer from 0 to 1,000,000.

Example:

```
qos marking dscp assign best-effort priority-method mapped-from-marking
qos marking precedence clear
qos max-link-bandwidth 500000
```

secondary

Description: Configure a secondary network on the interface.

Syntax:

secondary address

address must be one of these options: *addr mask* or *net*

- *addr* is an IP address, and must be in the format of A.B.C.D.
- *mask* is an IP subnet mask, and must be in the format of A.B.C.D.
- *net* is the IP address and subnet prefix in the format of A.B.C.D/# where # must be in the range of 0 to 32.

This command can take multiple address entries.

Use no **secondary** to remove all secondary addresses from this interface.

Example:

```
secondary 100.100.101.0 255.255.255.0
secondary 100.100.101.0/24
secondary 100.100.101.0/24 100.100.103.0/24
```

type

Description: Set the interface type.

Syntax:

type option

option must be one of these options: *trusted*, *optional*, *external* addressmethod

If **option** value is *external*, you must add the parameter addressmethod whose value is: *default-gw gateway*, *dhcp*, or *pppoe*.

- If addressmethod is *default-gw*, you must add the parameter gateway.
- gateway is IP address and subnet prefix of the default gateway in the format of A.B.C.D/#, where # must be in the range of 0 to 32.

Example:

```
type trusted
type external default-gw 100.100.101.0/24
```

vpn-pmtu

Description: Configure PMTU settings for IPsec for an external interface.

Syntax:

vpn-pmtu minimum-size size life-time time

size is the minimum MTU in bytes from 68 to 1550; default is 512.

time is the aging time of learned PMTU in seconds from 60 to 2147483647; default is 600.

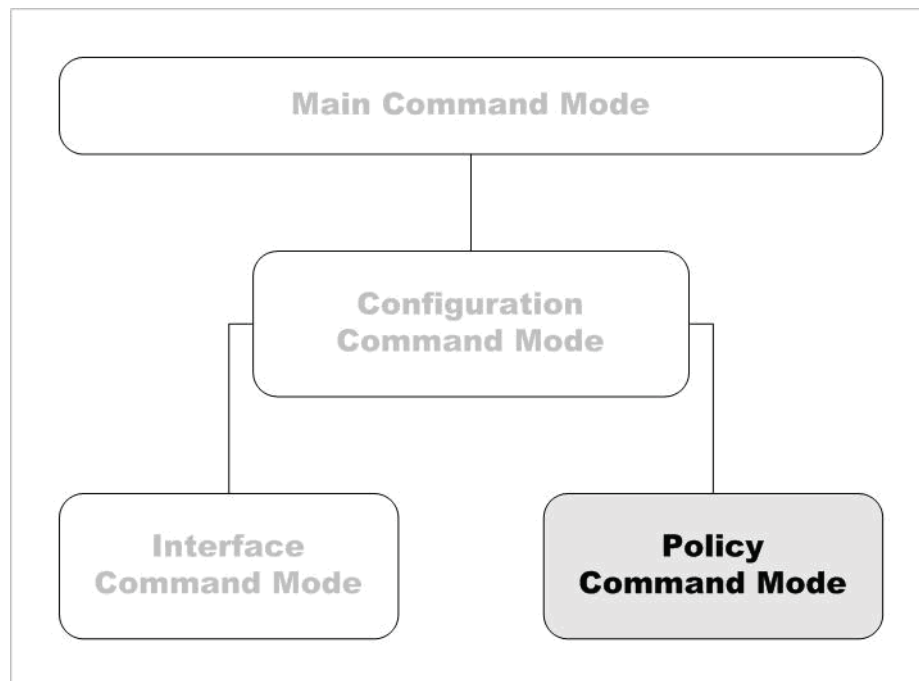
Example:

```
vpn-pmtu minimum-size 768 life-time 1200
```

7

Policy Command Mode

The WatchGuard Command Line Interface (CLI) Policy command mode is used to configure the firewall policies.



In the Policy mode, the administrator can:

- Create and modify rules and schedules
- Manage user accounts
- Define user, groups and aliases for use in policies
- Control branch office VPN gateways and tunnels
- Configure branch office and mobile user VPN policies

Enter the Policy Command Mode

To enter the Policy command mode:

- 1 Open the CLI in the Configuration command mode.
- 2 Type the **policy** command.
- 3 Press **Enter**.
The CLI prompt changes to WG(config/policy)#..

List of Policy Mode Commands

You can use all common commands in the Policy command mode. For more information, see “List of Common Commands” on page 15.

These commands are available only in the Policy mode:

Command	Usage
alias	Create aliases for a group of hosts, networks, or interfaces.
apply	Save a newly added or edited configuration.
auth-server	Configure authentication server settings.
auth-user-group	Define user groups for authentication.
bovpn-gateway	Configure a branch office VPN gateway policy.
bovpn-tunnel	Configure a branch office VPN tunnel policy.
dynamic-nat	Enable a dynamic NAT policy for traffic through specific interfaces.
mvpn-ipsec	Configure Mobile VPN with IPSec groups.
mvpn-rule	Configure Mobile VPN with IPSec policy rules.
one-to-one-nat	Enable the global use of 1-to-1 NAT to route traffic.
policy-type	Display a list of configured policies or the details of a specific policy.
pptp	Configure a Mobile VPN with PPTP policy.
proposal	Configure IPSec Phase 2 proposals.
rule	Configure security policy rules.
schedule	Create and modify a schedule to use in policies.
sslvpn	Configure the device to enable Mobile VPN with SSL.
traffic-management	Define traffic management actions to use in policies.
user-group	Create a user group to use in policies.
users	Add individual users to use in policy rules.

Policy Command Mode Reference

alias

Description: Create shortcuts to identify a group of hosts, networks, or interfaces.

Syntax:

alias name description desc option
<p>Configure an alias for a single device, network, or IP address range.</p> <p>name is the unique string that identifies the alias. You cannot use spaces.</p> <p>desc is a string that describes the use of the alias. You cannot use spaces.</p> <p>option must be one of these options: address, network-ip net, or host-range startip endip.</p> <ul style="list-style-type: none"> - address is the IP address of a device on the network. It must be in the format A.B.C.D. - net is the IP address of a device on the network. It must be in the format A.B.C.D./#, where # is a number from 0 to 32. - startip is the first IP address in the range. It must be in the format A.B.C.D. - endip is the last IP address in the range. It must be in the format A.B.C.D.
alias name description desc tunnel-address tunnel tunnelname address address user-group userdefinition
<p>Configure an alias for a tunnel to define the user or group, address, and tunnel name.</p> <p>name is the unique string that identifies the alias. You cannot use spaces.</p> <p>desc is a string that describes the use of the alias. You cannot use spaces.</p> <p>tunnelname is a string that identifies the tunnel.</p> <p>address must be one of these options: address, network-ip net, or host-range startip endip.</p> <ul style="list-style-type: none"> - address is the IP address of a device on the network. It must be in the format A.B.C.D. - net is the IP address of a device on the network. It must be in the format A.B.C.D./#, where # is a number from 0 to 32. - startip is the first IP address in the range. It must be in the format A.B.C.D. - endip is the last IP address in the range. It must be in the format A.B.C.D. <p>userdefinition defines a user or group for the tunnel. It is composed of usergroup groupname authmethod where:</p> <ul style="list-style-type: none"> - usergroup is either: <i>user</i> or <i>group</i>. - groupname is a string for a user or group as already defined on the device. - authmethod is one of these options: <i>Firebox-DB</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>SecurID</i>, or <i>Active-Directory</i>.
alias name description desc custom-address interface if-name address tunneladdress user-group userdefinition
<p>Configure an alias to define the user or group, address, and an interface on the device.</p> <p>name is the unique string that identifies the alias. You cannot use spaces.</p> <p>desc is a string that describes the use of the alias. You cannot use spaces.</p> <p>if-name is the name of the device interface.</p> <p>address must be one of these options: address, network-ip net, or host-range startip endip.</p> <ul style="list-style-type: none"> - address is the IP address of a device on the network. It must be in the format A.B.C.D. - net is the IP address of a device on the network. It must be in the format A.B.C.D./#, where # is a number from 0 to 32. - startip is the first IP address in the range. It must be in the format A.B.C.D. - endip is the last IP address in the range. It must be in the format A.B.C.D. <p>userdefinition defines a user or group for the tunnel. It is composed of usergroup groupname authmethod where:</p> <ul style="list-style-type: none"> - usergroup is either: <i>user</i> or <i>group</i>. - groupname is a string for a user or group as already defined on the device. - authmethod is one of these options: <i>Firebox-DB</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>SecurID</i>, or <i>Active-Directory</i>.

alias name description desc alias aliasname
<p>Configure an alias to another alias.</p> <p>name is the unique string that identifies the alias. You cannot use spaces.</p> <p>desc is a string that describes the use of the alias. You cannot use spaces.</p> <p>aliasname is an alias already configured on the device.</p>
alias name description desc user-group userdefinition
<p>Configure an alias to an authentication user or group.</p> <p>name is the unique string that identifies the alias. You cannot use spaces.</p> <p>desc is a string that describes the use of the alias. You cannot use spaces.</p> <p>userdefinition defines a user or group for the tunnel. It is composed of <i>usergroup groupname authmethod</i> where:</p> <ul style="list-style-type: none"> - <i>usergroup</i> is either: <i>user</i> or <i>group</i>. - <i>groupname</i> is a string for a user or group as already defined on the device. - <i>authmethod</i> is one of these options: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory</i>.

Example:

```
alias ceo description jacks_box host-ip 192.168.100.23
alias tunnel_mainoffice tunnel-address tunnel headquarters address network-ip
192.168.200.0/24
alias moneyfolk user-group group accounting Active-Directory
```

apply

Description: Apply configuration changes to the device.

Syntax:

apply
No options available.

auth-server

Description: Configure the device to use an authentication server.

Syntax:

```
auth-server type primary enable primaryIP secondary enable secondaryIP search-base
deadtime deadtimevalue dns-string dnsstring group-string groupstring idle-timeout-string
idletimeout ip-string ipstring lease-time-string leasetimestring login-attribute login netmask-
string netmask password passwd port portnumber wins-string wins
```

Configure the device to use either an LDAP or Active-Directory authentication server.

type must be one of these options: *LDAP* or *Active-Directory*.

primaryIP is the IP address of the primary authentication server. It must be in the format A.B.C.D.

secondaryIP is the IP address of the secondary authentication server. It must be in the format A.B.C.D.

search-base is the limits on the authentication server directories where the WatchGuard device searches for an authentication match.

For example, if your user accounts are stored in an OU (organizational unit) you refer to as accounts, you want to limit the search to only this OU, and your domain name is mydomain.com, your search base is: *ou=accounts,dc=mydomain,dc=com*

deadtimevalue is the duration in minutes before a dead server is marked as active again. It must be an integer from 0 to 1440. The default value is 10.

dnsstring is the distinguished name of a search operation. The maximum number of characters is 255.

groupstring is an attribute on an LDAP server that holds user group information. The maximum number of characters is 31.

idletimeout is the amount of time that can pass before an idle Mobile VPN user is removed from the authenticated user group. It must be an integer.

ipstring is a virtual IP address assigned to Mobile VPN clients. It must be in the format A.B.C.D.

leasetimestring controls the absolute amount of time a user can stay authenticated.

login is the name used for the bind to the LDAP database.

netmask is the network mask used with *ipstring* to define a virtual IP address for assignment to Mobile VPN clients.

passwd is the password of the searching user.

portnumber is the port used to connect to the authentication server. The default value is 389.

wins is an IP address for a WINS server assigned to Mobile VPN clients.

```
auth-server type primary enable primaryIP secret1 secondary enable secondary IP secret2
deadtime deadtimevalue group groupnumber port portnumber retry retries timeout
timeoutvalue
```

Configure the device to use a RADIUS or SecurID authentication server.

type must be one of these options: *RADIUS* or *SecurID*.

primaryIP is the IP address of the primary authentication server. It must be in the format A.B.C.D.

secondaryIP is the IP address of the secondary authentication server. It must be in the format A.B.C.D.

secret1 is the shared secret between the device and the primary authentication server.

secret2 is the shared secret between the device and the secondary authentication server.

deadtimevalue is the amount of time in minutes before a dead server is marked as active again. It must be an integer from 0 to 86400. The default value is 10.

groupnumber is the Group Attribute value. It must be an integer from 0 to 255. The default value is 11.

portnumber is the port used to connect to the authentication server. It must be an integer from 1 to 65535. The default value is 1812.

retries is the number of times the device tries to reconnect to the server before marking it inactive. It must be an integer from 1 to 10. The default value is 3.

timeoutvalue is the duration in seconds the device waits for a response from the authentication server before it tries to connect again. It must be an integer from 1 to 120. The default value is 5.

Example:

```
auth-server Active-Directory primary enable 192.168.110.5 secondary enable
192.168.110.6
auth-server RADIUS primary enable 192.168.110.5 authpassword deadtime 15
group 12 port 1813 retry 5 timeout 10
auth-server RADIUS secondary enable 192.168.110.6 auth2password deadtime 15
group 12 port 1813 retry 5 timeout 15
```

auth-user-group

Description: Create authentication users and groups in the Firebox internal database.

Syntax:

auth-user-group <i>name type server desc</i>
Define an authentication group or single user. <i>name</i> is a string to uniquely identify the authentication group or user. <i>type</i> must be either: <i>user</i> , or <i>group</i> . <i>server</i> must be one of these options: <i>Firebox-DB</i> , <i>LDAP</i> , <i>RADIUS</i> , <i>Active-Directory</i> , or <i>SecurID</i> . - <i>desc</i> is a string that describes the authentication group or user.

Example:

```
auth-user-group jackp user Chief_Executive_Officer
auth-user-group executives group VIPs
```

bovpn-gateway

Description: Configure a branch office virtual private network (BOVPN) gateway.

Syntax:

bovpn-gateway name

Assign a unique name to a BOVPN gateway.

name is a string that uniquely identifies the BOVPN gateway.

After you enter the command **bovpn-gateway name** the configuration continues to the BOVPN Gateway details command.

The prompt changes to “WG(config/policy/bovpngateway-*name*)#”.

Use the **Exit** command to exit this mode.

endpoint rgateway rgatewayid lgatewayid interface authentication

Configure the general settings for a BOVPN gateway. At first, this is the only command available. After you configure a gateway other commands become available.

name is the gateway name. The maximum number of characters is 124.

rgateway must be either: *dynamic* or **rem-ip-address**.

- **rem-ip-address** is an IP address for the remote gateway in the format A.B.C.D.

rgatewayid must be either: **rem-ip-address** or *by-domain method domainname resolvable*.

- **rem-ip-address** is an IP address for the remote gateway in the format A.B.C.D.
- **method** is one of these options: *domain-name*, *user-domain*, or *x500*.
- **domainname** is the string that represents the domain name.
- *resolvable* determines whether the device attempts to resolve the domain name. The value must be one of these options: *yes* or *no*. Specify *yes* if the domain name is resolvable or *no* if it is not.

lgatewayid must be either: **loc-ip-address** or *by-domain method domainname*.

- **loc-ip-address** is an IP address for the local gateway in the format A.B.C.D.
- **method** is one of these options: *domain-name* or *user-domain*.
- **domainname** is the string that represents the domain name.

interface is the alias of the external interface used for the local gateway.

authentication is the method used to secure the tunnel. It must be either: **certificate** or **preshared**

- **certificate** is in the form of: **certificate id type algorithm name** where:
 - * **id** is the certificate identification number.
 - * **type** must be one of these options: *none*, *ip-address*, *domain*, *user-domain*, or *x500*.
 - * **algorithm** is either: *rsa* or *dsa*.
 - * **name** is the certificate name.
- **presharedkey** is in the form of: **pre-shared secret**, where **secret** is the shared secret used to negotiate the tunnel.

auto-start enable

Configure the BOVPN tunnel to start negotiation as soon as the device restarts.

No options available.

certificate id type algorithm name

Edit device IPSec certificate used in BOVPN.

id is the certificate identification number.

type must be one of these options: *none*, *ip-address*, *domain*, *user-domain*, or *x500*.

algorithm is either: *rsa* or *dsa*.

name is the certificate name.

phase1 attribute

Add or edit phase 1 configurations for BOVPN.

attribute is one of these options:

- **p1-attrib enable**
 - * **p1-attrib** is one of these options: *dead-peer-detection*, *ike-keep-alive*, or *nat-traversal*.
- **dpd-max-retries tries traffic-idle-timeout time**
 - * **tries** is an integer from 1 to 30.
 - * **time** is an integer from 10 to 300.
- **keep-alive-interval k-time**
 - * **k-time** is an integer from 1 to 65535. The IKE keep-alive interval for NAT traversal.
- **max-failures count**
 - * **count** is an integer from 1 to 30. The maximum number of failures that can occur before BOVPN no longer sends IKE keep-alive messages.
- **message-interval mi-time**
 - * **mi-time** is an integer from 0 to 300. The message interval for IKE keep-alive.
- **mode gw-mode**
 - * **gw-mode** is the gateway mode. It must be one of these options: *Main*, *Aggressive*, or *Main-Fallback-Aggressive*.
- **transform index method encrypt life group**
 - * **index** is the transform index to edit the previously configured transform settings.
 - * **method** is either: *MD5*, or *SHA1*.
 - * **encrypt** is one of these options:
 - *DES life unit t-unit*
 - *DES-3 life unit t-unit*
 - *AES life encrypt-key-length length unit t-unit*
 where:
 - **life** is the SA life
 - **length** is the AES encryption key length
 - **t-unit** is either: *minute*, or *hour*
 - * **group** is one of these options: *Diffie-Hellman-Group1*, *Diffie-Hellman-Group2*, or *Diffie-Hellman-Group5*

pre-shared secret

Edit the pre-shared secret key for the BOVPN.

secret is the shared secret used to negotiate the tunnel.

Example:

```
bovpn-gateway Headquarters
endpoint 202.58.165.10 202.58.165.10 216.129.32.20 External pre-shared
n0s3cr3+!
phase1 transform MD5 DES 120 encrypt-key-length 16 unit hour Diffie-Hellman-
Group1
pre-shared mys3cr3tk3y
```

bovpn-tunnel

Description: Create or modify a tunnel for a branch office virtual private network.

Syntax:

bovpn-tunnel *name*

Assign a unique name to a BOVPN tunnel.

name is a string that uniquely identifies the BOVPN tunnel.

After you type the command **bovpn-gateway *name*** the configuration continues to the BOVPN Tunnel details command.

The prompt changes to “WG(config/policy/bovpntunnel-*name*)#”.

Use the **Exit** command to exit this mode.

gateway *gateway localaddress remoteaddress direction enable-broadcast*

Configure tunnel route settings for a gateway already configured on the device. After you enter the gateway command, other BOVPN Tunnel commands become available. At first, ***localaddress*** and ***remoteaddress*** are required fields, but when you edit a tunnel these fields are no longer required.

gateway is the gateway name.

localaddress must use one of these formats:

- **host *ipaddress*** where ***ipaddress*** is an IP address for the local end point in the format A.B.C.D.
- **range *start-ip startip end-ip endip*** where:
 - * ***startip*** is the first IP address of a range in the format A.B.C.D.
 - * ***endip*** is the last IP address of a range in the format A.B.C.D.
- **subnet *net*** where ***net*** is a network address and mask in the format A.B.C.D./#.

remoteaddress must use one of these formats:

- **host *ipaddress*** where ***ipaddress*** is an IP address for the local end point in the format A.B.C.D.
- **range *start-ip startip end-ip endip*** where:
 - * ***startip*** is the first IP address of a range in the format A.B.C.D.
 - * ***endip*** is the last IP address of a range in the format A.B.C.D.
- **subnet *net*** where ***net*** is a network address and mask in the format A.B.C.D./#

direction sets the direction of the traffic through the tunnel. You must use one of these options:

- ***bi-direction nat-type*** — traffic routed both ways through the tunnel (default).
- ***inbound nat-type*** — traffic routed from the remote address to the local address.
- ***outbound nat-type*** — traffic routed from the local address to the remote address.
- * ***nat-type*** must be ***type ip-address*** where:
 - type*** is one of these options:
 - ~ ***dnat*** — Dynamic NAT IP address for either inbound or outbound only.
 - ~ ***host-ip*** — 1-to-1 NAT host IP address.
 - ~ ***network-ip*** — 1-to-1 NAT network IP address.
 - ~ ***range-ip*** — 1-to-1 range of IP addresses.
 - ~ ***ip-address*** is in the format A.B.C.D. or A.B.C.D/(0 to 32) whichever is applicable.

enable-broadcast must be ***broadcast-over-tunnel enable*** to enable Broadcast over BOVPN.

add-to-policy *enable*

Add the tunnel to the BOVPN-Allow policies.

No options available.

address-pair *index localaddress remoteaddress direction enable-broadcast*

Add or edit an address pair of the tunnel.

index is the index of the address pair to be edited.

localaddress must use one of these formats:

- **host *ipaddress*** where ***ipaddress*** is an IP address for the local end point in the format A.B.C.D.
- **range *start-ip startip end-ip endip*** where:
 - * ***startip*** is the first IP address of a range in the format A.B.C.D.
 - * ***endip*** is the last IP address of a range in the format A.B.C.D.
- **subnet *net*** where ***net*** is a network address and mask in the format A.B.C.D./#.

remoteaddress must use one of these formats:

- **host *ipaddress***, where ***ipaddress*** is an IP address for the local end point in the format A.B.C.D.
- **range *start-ip startip end-ip endip*** where:
 - * ***startip*** is the first IP address of a range in the format A.B.C.D.
 - * ***endip*** is the last IP address of a range in the format A.B.C.D.
- **subnet *net*** where ***net*** is a network address and mask in the format A.B.C.D./#.

direction sets the direction of the traffic through the tunnel. You must use one of these options:

- ***bi-direction nat-type*** — traffic routed both ways through the tunnel (default)
- ***inbound nat-type*** — traffic routed from the remote address to the local address
- ***outbound nat-type*** — traffic routed from the local address to the remote address
- * ***nat-type*** must be ***type ip-address*** where ***type*** is one of these options:
 - ***dnat*** — Dynamic NAT IP address for either inbound or outbound only.
 - ***host-ip*** — 1-to-1 NAT host IP address.
 - ***network-ip*** — 1-to-1 NAT network IP address.
 - ***range-ip*** — 1-to-1 NAT range of IP addresses.
 - ***ip-address*** is in the format A.B.C.D. or A.B.C.D/(0 to 32), whichever is applicable.

enable-broadcast must be ***broadcast-over-tunnel enable*** to enable Broadcast over BOVPN.

move *where*

Move the tunnel either up, down, or to a certain indexed location.

where must be one of these options:

- ***up index1***
- ***down index1***
- ***to index2***

index1 or ***index2*** is the arbitrary location to which the tunnel moves. If ***index1*** is omitted it is understood to be a value of 1.

multicast-settings enable *origin-ip group-ip direction*

Configure the tunnel to allow multicast packets.

origin-ip is the origination IP address of the multicast.

group-ip is the multicast address of the receiving hosts.

direction is either:

- ***input if-index*** — where ***if-index*** is the interface index of one of the trusted or optional interfaces, where the multicast origin host is connected.
- ***input if-index if-index*** — where ***if-index*** is the interface index or indexes of the trusted or optional interfaces, where the receiving hosts are connected.

When Multicast is enabled, the command `tunnel-endpoints` must be used to define the route for encapsulation.

phase2 pfs enable *group*

Enable Perfect Forwarding Secrecy of the tunnel.

group is the IKE Diffie-Hellman group. It must be one of these options: *dh-group1*, *dh-group2*, or *dh-group5*.

phase2 proposals *p2name*

Assign a Phase 2 proposal to the tunnel.

p2name is an existing Phase 2 proposal on the device.

tunnel-endpoints *local-ip remote-ip*

Define the route for encapsulation of broadcast and multicast traffic.

Used only when one or both of these options are enabled: Broadcast or Multicast.

local-ip is the unused IP address on the local network of the tunnel address pair.

remote-ip is the unused IP address on the remote network of the tunnel address pair.

Example:

```
bovpn-tunnel SeattleNewYork
gateway GWSeattleNewYork network-ip 192.168.111.0/24 network-ip 10.10.10.0/24
broadcast-over-tunnel enable
gateway GWSeattleNewYork network-ip 192.168.111.0/24 network-ip 10.10.10.0/24
outbound dnat 172.16.30.5
```

dynamic-nat

Description: Configure the device to use dynamic network address translation.

Syntax:**dynamic-nat from *local* to *remote***

local is a host address, host range, network, or alias for a location on the protected network.

remote is a host address, host range, network, or alias for a location outside of the protected network.

Example:

```
dynamic-nat from webservers to Any-External
```

mvpn-ipsec

Description: Configure a device to use Mobile User VPN with IPsec.

Syntax:

mvpn-ipsec name

name is the group name of an existing Mobile VPN with IPsec configuration.
Use `no mvpn-ipsec name` to disable.

After you type the command `mvpn-ipsec name`, the CLI continues to the initial Mobile VPN with IPsec configuration command.

The prompt changes to "`WG(config/policy/muvpn-name)#`".

Use the **Exit** command to exit this mode.

auth-server auth-svr authmethod is-force-all ip-pool

Set initial configuration of Mobile VPN with IPsec.

auth-svr is the authentication server used for Mobile VPN with IPsec. It must be one of these options: *Firebox-DB*, *RADIUS*, *LDAP*, *Active-Directory*, or *SecurID*.

authmethod is the authentication method used for the tunnel. Must be one of these options:

- **rsa-svr-IP admin-passphrase**
 - * **rsa-svr-IP** is the RSA certificate server IP address.
 - * **admin-passphrase** is the administrator passphrase of the RSA server.
- **tunnel-passphrase** is the tunnel encryption passphrase.

is-force-all is a boolean to denote if it is a Captive Tunnel or Split Tunnel. Must be one of these options: *no tunnel-resource* or *yes*

- **tunnel-resource** is the address of the allowed resource in the format: **hostip** or **network-ip**
 - * **hostip** is an IP address in the format A.B.C.D.
 - * **network-ip** is a network address and mask in the format A.B.C.D./#, where # is a number from 0 to 32.

ip-pool is the address to assign to mobile computers that connect with Mobile VPN with IPsec.

The address has the format: *host-ip hostip* or *range-ip start-ip end-ip*

- **hostip** is an IP address in the format A.B.C.D.
- **start-ip** is the start of a range of IP addresses in the format A.B.C.D.
- **end-ip** is the end of a range of IP addresses in the format A.B.C.D.

After you type the command **auth-server auth-svr auth-method is-force-all ip-pool** the CLI continues to the detailed Mobile VPN with IPsec configuration command. This enables you to edit the initial configuration if you do not want to use the default values. You must use the **Apply** command before your changes are enabled. Use the **Exit** command to exit this mode..

all-traffic-allow enable
Force all traffic through the tunnel. Use no all-traffic-allow tunnel-resource to disable this command. <ul style="list-style-type: none"> - tunnel-resource is the address of the allowed resource in the format: hostip or network-ip * hostip is an IP address in the format A.B.C.D. * network-ip is a network address and mask in the format A.B.C.D./#, where # is a number from 0 to 32.
auth-method authmethod timeout
Configure or edit the authentication method. authmethod is the authentication method used for the tunnel. It must be one of these options: <ul style="list-style-type: none"> - rsa-svr-IP admin-passphrase * rsa-svr-IP is the RSA certificate server IP address. * admin-passphrase is the administrator passphrase of the RSA server. - tunnel-passphrase is the tunnel encryption passphrase. timeout is the time in seconds before the certificate authority request times out. It must be an integer from 0 to 600; default is 25.
auth-server auth-svr
Set or replace the authentication server. auth-svr is the authentication server used for Mobile VPN with IPsec. It must be one of these options: <i>Firebox-DB</i> , <i>RADIUS</i> , <i>LDAP</i> , <i>Active-Directory</i> , or <i>SecurID</i> .
firebox-ip primary primary-ip backup backup-ip
Set the primary and backup IP address of the WatchGuard device or remove the backup IP address used in Mobile VPN with IPsec. primary-ip is the primary external interface IP address. backup-ip is the secondary external interface IP address. You can use the command no firebox-ip backup to delete only the backup WatchGuard device IP address.
line-management mode timeout
Set line management, for users with Mobile VPN with IPsec client software v10 or later. mode is any of these options: <i>manual</i> , <i>automatic</i> , or <i>variable</i> . timeout is an integer from 0 to 65535.
phase1 setting
Set or modify the Phase 1 settings. setting is one of these options: <ul style="list-style-type: none"> - authentication authmethod where authmethod must be either: <i>MD5</i> or <i>SHA</i> - encryption encrypmethod where encrypmethod must be: <i>DES</i>, <i>TRIPLE-DES</i>, <i>AES-128</i>, <i>AES-192</i>, or <i>AES-256</i> - sa-life duration unit unittype * duration is an integer from 0 to 2147483647. * unittype is either: <i>hour</i> or <i>minute</i>. - key-group grouptype where grouptype must be: <i>dh-group1</i>, <i>dh-group2</i>, or <i>dh-group5</i>. - nat-traversal enable interval where interval is an integer from 0 to 2147483647. - ike-keep-alive enable interval max-failures * interval is an integer from 0 to 300. * max-failures is an integer from 1 to 30. - dpd enable timeout max-retries * timeout is an integer from 10 to 300. * max-retries is an integer from 1 to 30.

<p>phase2 setting</p> <p>Set or modify a Phase 2 settings.</p> <p>setting is one of these options:</p> <ul style="list-style-type: none"> - authentication <i>authmethod</i> where <i>authmethod</i> must be either: <i>MD5</i> or <i>SHA</i>. - encryption <i>encrypmethod</i> where <i>encrypmethod</i> must be: <i>None</i>, <i>DES</i>, <i>TRIPLE-DES</i>, <i>AES-128</i>, <i>AES-192</i>, or <i>AES-256</i>. - key-expiration-time enable <i>lifetime kbytes unittype</i> <ul style="list-style-type: none"> * <i>lifetime</i> is an integer from 0 to 2147483647; default is 8. * <i>kbytes</i> is an integer from 1 to 2147483647. * <i>unittype</i> is either <i>hour</i> or <i>minute</i>. - pfs enable <i>group</i> <ul style="list-style-type: none"> * <i>group</i> is one of these options: <i>dh-group1</i>, <i>dh-group2</i>, or <i>dh-group5</i>.
<p>resource-addr tunnel-resource</p> <p>Specify the allowed resources for Mobile VPN with IPSec.</p> <p>tunnel-resource is the address of the allowed resource in the format: hostip or network-ip</p> <ul style="list-style-type: none"> - hostip is an IP address in the format A.B.C.D. - network-ip is a network address and mask in the format A.B.C.D./# where # is a number from 0 to 32.
<p>timeouts option time</p> <p>Set the session and idle timeouts. If the authentication server is also configured with these timeouts, the server configuration takes precedence over these settings</p> <p>option is either <i>idle</i> or <i>session</i>.</p> <p>time is the idle or session timeout in minutes, an integer from 0 to 43200.</p>
<p>virtual-addr ip-pool</p> <p>Set the IP address pool that is assigned to mobile computers that connect with Mobile VPN with IPSec.</p> <p>ip-pool is the pool of IP addresses in the format: host-ip hostip or range-ip start-ip end-ip</p> <ul style="list-style-type: none"> - hostip is an IP address in the format A.B.C.D. - start-ip is the start of a range of IP addresses in the format A.B.C.D. - end-ip is the end of a range of IP addresses in the format A.B.C.D.

Example:

```

mvpn-ipsec MVPNIPSecUsers
auth-server Firebox-DB mypassphraze3 yes host-ip 192.168.113.100
resource-addr host-ip 192.168.110.86
virtual-addr range-ip 192.168.100.50 192.168.100.100
    
```

mvpn-rule

Description: Configure Mobile User VPN with IPsec policy rules.

Syntax:

mvpn-rule *name*

name is the rule name to assign to the Mobile VPN IPsec policy rules.
Use `no mvpn-rule name` to delete rule.

After you type the command `mvpn-rule name`, the CLI continues to the selection of the Mobile VPN with IPsec group to which the Mobile VPN rules are applied.

The prompt changes to “WG(config/policy/mvpnrule-*name*)#”.

Use the **Exit** command to exit this mode.

mvpn-ipsec *name policy-type*

Select the Policy Type to be applied to the Mobile VPN with IPsec group.

name is the existing Mobile VPN with IPsec group name to which the rule is applied.
policy-type is the pre-defined Policy Types assigned to the rule.

After you enter the command `mvpn-ipsec name policy-type`, a range of new commands is available to configure the rule details. You must use the **Apply** command to enable your changes.

option enable

Enable Mobile VPN with IPsec rule options.

option must be one of these options:

- *auto-block* — auto block external sites that attempt to connect.
- *icmp-message allow-all* — permit all ICMP error messages.
- *icmp-message fragmentation-required* — fragmentation is required, but DF bit is set.
- *icmp-message host-unreachable* — the send host is unreachable.
- *icmp-message network-unreachable* — the send network is unreachable.
- *icmp-message port-unreachable* — the send port is unreachable.
- *icmp-message protocol-unreachable* — the send protocol is unreachable.
- *icmp-message time-exceeded* — the time to live is exceeded in transit.
- *icmp-message use-global* — use global settings in the response.

firewall action

action must be one of these options: *allowed*, *denied*, or *reject* **option**.

- If you select the *reject* action, **option** must be added as one of these options: *ICMP_HOST*, *ICMP_NETWORK*, *ICMP_PORT*, *ICMP_PROTOCOL*, or *TCP_RST*.

idle-time

Specify the custom idle timeout for the rule.

time timeout in seconds. This must be an integer from 0 to 2147483647. A value of 0 disables this function.

logging option

Configure logging settings specific to the rule.

option must be one of these options:

- *log-message enable* — send log message.
- *snmp-trap enable* — send SNMP trap.
- *notification enable action-type type launch-interval interval repeat-count count* — send notification, where:
 - * **type** is either *email* or *pop-window*. The default is *email*.
 - * **interval** is the launch interval in minutes from 1 to 65535. The default is 15.
 - * **count** is the repeat count; an integer from 1 to 256. The default is 10.

proxy-action <i>action</i>
Apply the matching default proxy actions for the rule. <i>action</i> must be one of these options: <i>DNS-Outgoing, DNS-Incoming, FTP-Client, FTP-Server, HTTP-Client, HTTP-Server, POP3-Client, POP3-Server, SMTP-Outgoing, SMTP-Incoming, TCP-UDP-proxy, H.323-Client, SIP-Client, DNS-Incoming, HTTPS-Client, or HTTPS-Server.</i>
qos enable
Override QoS settings for an interface if Traffic Management and QoS are enabled. No available options.
qos marking <i>type method priority-method p-method</i>
<i>type</i> must be either <i>dscp</i> or <i>precedence</i> . <i>method</i> must be either <i>assign m-value</i> or <i>preserve</i> . <ul style="list-style-type: none"> - If <i>type</i> is <i>dscp</i>, <i>m-value</i> is one of these options: <i>Best-effort, CS1-Scavenger, AF11, AF12, AF13, CS2, AF21, AF22, AF23, CS3, AF31, AF32, AF33, CS4, AF41, AF42, AF43, CS5, EF, Control-CS6, or Control-CS7.</i> - If <i>type</i> is <i>precedence</i>, <i>m-value</i> is an integer from 0 (normal) to 7 (highest). <i>p-method</i> is a string. It must be one of these options: <i>No_Priority, Customized c-value, Mapped-from-Marking.</i> <i>c-value</i> is an integer from 0 (normal) to 7 (highest).
schedule <i>sked-name</i>
Assign an existing schedule to the policy. <i>sked-name</i> is the schedule that was already created.
specify-user <i>name auth-svr</i>
Assign a specific user to the policy. <i>name</i> is an existing user name. <i>auth-svr</i> must be one of these options: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory.</i>
traffic-mgmt <i>tm-name</i>
Assign an existing traffic management action to the policy. <i>tm-name</i> is the traffic management rule that was already created.

Example:

```

mvpn-rule MVPNIPSecRule1
mvpn-ipsec MVPNIPSecUsers HTTP-proxy
logging notification enable action-type email launch-interval 10 repeat-count
50
qos marking dscp assign AF11 priority-method Customized 5
schedule wkdays-only
    
```

one-to-one-nat

Description: Create a 1-to-1 NAT table.

Syntax:

```
one-to-one type nataddress realaddress interface
```

type must be one of these options: *host*, *subnet*, or *range*.
nataddress is the address visible to the insecure network.
realaddress is the real address on the protected network.
interface is the name of the interface used for 1-to-1 NAT.

Example:

```
one-to-one host 203.28.18.2 192.168.110.24 External
```

policy-type

Description: Create a custom policy template.

Syntax:

```
policy-type name timeout protocol port
```

Create a custom policy template that can be used to create firewall policy actions.

name is a unique string to identify the policy template. You cannot use spaces.

timeout is the idle timeout in seconds. It must be an integer from 0 to 65535. The default is 180.

All ports are integers from 1 to 65535. **port** must be one of these options:

- **tcp port-range firstport lastport**
- **tcp port**
- **udp port-range firstport lastport**
- **udp port**
- **gre**
- **ah**
- **esp**
- **any**
- **icmp type code**

* **type** must be: *Echo_Reply*, *Destination_Unreachable*, *Source_Quench*, *Redirect*, *Echo_Request*, *Time_Exceeded*, *Parameter_Problem*, *Timestamp_Request*, *Timestamp_Reply*, *Information_Request*, *Information_Reply*, *Address_Mask_Request*, *Address_Mask_Reply*, or *Any*.

* **code** must be an integer from 0 to 255.

Example:

```
policy-type funkydb.1 protocol udp 60002
```

pptp

Description: Configure the firewall to allow Mobile VPN with PPTP.

Syntax:

pptp enable
No options available. Use no pptp enable to disable Mobile VPN with PPTP.
pptp setting value
Set maximums in bytes. setting must be either: <i>pptp-mtu</i> or <i>pptp-mru</i> value must be an integer from 500 to 1500. The default is 1400.
pptp pptp-address address
Define the PPTP address pool. address must be either host ipaddress or range firstip lastip . ipaddress , firstip , and lastip are all IP addresses with the format A.B.C.D.
pptp option
Enable PPTP options. option must be one of these options: auth-domain domain where domain is the authentication domain name. auth-session-timeout session where session is an integer from 0 to 43200. The default is 12. auth-idle-timeout idle where idle is an integer from 0 to 43200. The default is 15. mppe method where method must be: <i>encryption-128-bits</i> , <i>enable-fallback-to-40-bits</i> , or <i>no encryption</i> .

Example:

```
pptp pptp-mtu 1500
pptp pptp-address range 192.168.110.100 192.168.110.140
pptp auth-session 20
```

proposal

Description: Create Phase 2 proposals for IPSec VPN.

Syntax:

proposal p2 p2name p2type transform life-time life-size encryption authentication
Configure the Phase 2 proposal details. p2name is a unique string to identify the IPSec Phase 2 proposal. p2type is the Phase 2 proposal type. It must be either <i>ah</i> , or <i>esp</i> . life-time is the SA life time in minutes from 1 to 2147483647. life-size is the SA life size in kilobytes from 1 to 2147483647. encryption is the encryption algorithm for Encapsulated Security Payload (ESP) type only. If type is Authentication Header (AH) this argument is omitted. It must be one of these options: <i>none</i> , <i>des</i> , <i>3des</i> , <i>aes128</i> , <i>aes192</i> , or <i>aes256</i> . authentication is the authentication algorithm. For AH proposal type authentication is either <i>md5</i> or <i>sha1</i> . For ESP, it must be one of these options: <i>none</i> , <i>md5</i> , or <i>sha1</i> .
proposal p2 p2name replay-detection size
Set the anti-replay window size. p2name is a unique string to identify the IPSec Phase 2 proposal. size is the window size of the replay detection. It must be one of these options: <i>disable</i> , <i>window-32</i> , or <i>window-64</i> .

Example:

```
proposal p2 p2esp esp transform 480 1024 aes256 md5
proposal p2 p2ah ah transform 1440 2048 sha1
proposal p2 p2ah replay-detection window-32
```

rule

Description: Configure the rules of the security policy.

Syntax:

rule name
<p>name is the policy name on the firewall. Use <code>no rule name</code> to delete rule.</p>

After you type the command **rule name** the CLI continues to the policy type assignment of the rule.

The prompt changes to “WG(config/policy/rule-name)#”.

Use the **Exit** command to exit this mode.

policy-type p-type from source to destination
<p>Select the Policy Type to be applied to the rule.</p> <p>p-type is the policy type. To see the list of policy types you can execute the command <code>show policy-type</code>.</p> <p>source is one or more of these options:</p> <ul style="list-style-type: none"> - <i>alias if-alias</i> — if-alias is the interface alias. It must be one of these options: <i>Trusted, Optional, External, Any-Trusted, Any-Optional, or Any-External</i>. - <i>custom-address if-alias address address-format group-user type name authsvr</i> * address-format must be one of these options: <ul style="list-style-type: none"> • <i>host-ip A.B.C.D</i> • <i>host-range A.B.C.D W.X.Y.Z</i> • <i>network-ip A.B.C.D/M</i> * type is either <i>user</i> or <i>group</i>. * name is the user name or group name. * authsvr is one of these options: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory</i>. - <i>tunnel-address bovpn</i> — bovpn is the BOVPN name. - <i>user-group type name authsvr</i> <p>destination is one or more of these options:</p> <ul style="list-style-type: none"> - <i>alias if-alias</i> — if-alias is the interface alias. It must be one of these options: <i>Trusted, Optional, External, Any-Trusted, Any-Optional, or Any-External</i>. - <i>custom-address if-alias address address-format group-user type name authsvr</i> * address-format must be one of these options: <ul style="list-style-type: none"> • <i>host-ip A.B.C.D</i> • <i>host-range A.B.C.D W.X.Y.Z</i> • <i>network-ip A.B.C.D/M</i> * type is either <i>user</i> or <i>group</i>. * name is the user name or group name. * authsvr is one of these options: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory</i>. - <i>tunnel-address bovpn</i> — bovpn is the BOVPN name. - <i>user-group type name authsvr</i> <p>is-enable denotes if the rule is active or not. It must be either <i>enable</i> or <i>disable</i>.</p>

After you type the command **policy-type p-type from source to destination is-enable** a new range of commands is available to configure the rule details. You must use the **Apply** command to enable your changes.

<p>alarm alarmid trap remote action launch-interval repeat-count block</p> <p>Configure an alarm for the specified rule.</p> <p>name is the name of the rule.</p> <p>alarmid is an alarm identification.</p> <p>trap enables an SNMP trap. The value must be either <i>0</i> or <i>1</i>.</p> <p>remote enable notification. The value must be either <i>0</i> or <i>1</i>.</p> <p>action sets the notification type. It must be either <i>email</i> or <i>popup</i>.</p> <p>launch-interval is the minimum time in minutes between different notifications. It must be an integer from 60 to 3932100.</p> <p>repeat-count is the number of times an event can occur before an additional alarm is sent. It must be an integer from 1 to 256.</p> <p>block enables the automatic addition of the source IP to the blocked site. The value must be either <i>0</i> or <i>1</i>.</p>
<p>dynamic-nat switch</p> <p>Enable dynamic NAT for traffic controlled by the specified rule.</p> <p>switch must be one of these options:</p> <ul style="list-style-type: none"> - disable - enable function — where function is either: <ul style="list-style-type: none"> * <i>network-nat-setting</i> * <i>all-traffic-in-policy ip-address</i> — where ip-address is in the format A.B.C.D.
<p>firewall action</p> <p>Set the firewall action for the specified rule.</p> <p>action must be one of these options: <i>Allowed</i>, <i>Denied</i> switch, or <i>Reset</i> resetaction switch</p> <ul style="list-style-type: none"> - switch is either: <i>enable</i>, or <i>disable</i>. - resetaction must be one of these options: <i>Disabled</i>, <i>ICMP_HOST</i>, <i>ICMP_NETWORK</i>, <i>ICMP_PORT</i>, <i>ICMP_PROTOCOL</i>, or <i>TCP_RST</i>
<p>from source</p> <p>Edit the source field of an existing policy.</p> <p>source is any or a combination of these options:</p> <ul style="list-style-type: none"> - <i>alias if-alias</i> — if-alias is the interface alias. Must be one of these options: <i>Trusted</i>, <i>Optional</i>, <i>External</i>, <i>Any-Trusted</i>, <i>Any-Optional</i>, or <i>Any-External</i>. - <i>custom-address if-alias address address-format group-user type name authsvr</i> * address-format must be one of these options: <ul style="list-style-type: none"> • <i>host-ip A.B.C.D.</i> • <i>host-range A.B.C.D W.X.Y.Z.</i> • <i>network-ip A.B.C.D/M.</i> * type is either <i>user</i> or <i>group</i>. * name is the user name or group name. * authsvr is one of these options: <i>Firebox-DB</i>, <i>RADIUS</i>, <i>LDAP</i>, <i>SecurID</i>, or <i>Active-Directory</i>. - <i>tunnel-address bovpn</i> — bovpn is the BOVPN name. - <i>user-group type name authsvr</i>
<p>icmp-message action</p> <p>Set the traffic action for ICMP messages.</p> <p>action must be one of these options: <i>use-global</i>, <i>allow-all</i>, <i>deny-all</i>, or <i>option</i>.</p> <ul style="list-style-type: none"> - option can be any combination of these options: <i>fragmentation-required</i>, <i>time-exceeded</i>, <i>network-unreachable</i>, <i>host-unreachable</i>, <i>protocol-unreachable</i>, and <i>port-unreachable</i>.
<p>idle-timeout length</p> <p>Set the idle timeout in seconds.</p> <p>length is the idle timeout in seconds. It must be an integer from 0 to 2147483647.</p>

ips-monitor
Enable or disable the IPS-Monitor feature of the specified rule. <i>No options available.</i> Use no ips-monitor to disable the feature.
logging
Enable or disable logging for the specified rule. <i>No options available.</i> Use no logging to disable the feature.
move location
Move the policy to a numbered location. location is the desired location of the policy.
one-to-one-nat switch
Select whether to use 1-to-1 NAT for the policy. The default is to use 1-to-1 NAT. switch is either <i>0</i> (disable) or <i>1</i> (enable).
policy-routing backup primary-ext failover backup-ext backup-ext
Configure policy-based routing. primary-ext is the alias of the primary external interface for the policy. backup-ext is the alias of the backup external interface for the policy. You can assign more than one backup external interface to a policy.
proxy-action action
Assigned a default proxy action to a policy. action is the default proxy action on the device. To see the list of proxy actions, you can execute the command <code>show proxy-action</code> .
qos enable
For each interface, enable or disable the QoS feature of the specified rule. <i>No options available.</i> Use no qos enable to disable the feature.
qos marking dscp state priority-method method
For each interface, override QoS settings for the traffic controlled by the specified rule. state is the DSCP state and must be either assign type or <i>preserve</i> . type is the DSCP assign method and must be one of these values: <i>Best-effort, CS1-Scavenger, AF11, AF12, AF13, CS2, AF21, AF22, AF23, CS3, AF31, AF32, AF33, CS4, AF41, AF42, AF43, CS5, EF, Control-CS6, or Control-CS7</i> . method is the method used to assign priority, and must be one of these values: <i>No_Priority, Customer, or Mapped-from-Marking</i> .
rule name qos marking precedence state priority-method method
For each interface, override QoS precedence for the traffic controlled by the specified rule. state is the precedence state and must be either assign value or <i>preserve</i> . value is the precedence value. It must be an integer from 0 to 7. method is the method used to assign priority and must be one of these values: <i>No_Priority, Customer, or Mapped-from-Marking</i> .
schedule sked-name
Assign an existing schedule to the policy. sked-name is the schedule that was already created.

<p>server-load-balance external method sticky internal-ip weight port</p> <p>Configure policy-based server load balancing.</p> <p>external must be either:</p> <ul style="list-style-type: none"> - ip ipaddr, where ipaddress is in the format of A.B.C.D. - address nameexternal, where nameexternal is an alias for an external interface. <p>method must be either <i>round-robin</i> or <i>least-connection</i>.</p> <p>sticky is measured in minutes and must be an integer from 0 to 2147483647; select 0 for disabled. You can add from 2 to 10 internal servers to a policy. For each server, you must configure these options:</p> <ul style="list-style-type: none"> - internal-ip must be an address on the trusted or optional network in the format A.B.C.D. - weight is the priority assigned to the specified internal-ip, relative to the other configured servers. - port is the port number and must be an integer from 0 to 65535.
<p>snmp</p> <p>Enable or disable the send an SNMP trap feature of the specified rule.</p> <p><i>No options available.</i></p> <p>Use no snmp to disable the feature.</p>
<p>static-nat external internal port</p> <p>Configure the policy to use static NAT.</p> <p>external is either:</p> <ul style="list-style-type: none"> - ext-ip address, where address is an IP address on the external network in the format A.B.C.D. - ext-addr alias, where alias is a name or alias for an external network address. <p>internal is an IP address on the internal network in the format A.B.C.D.</p> <p>port is the port used to connect, and must be an integer from 0 to 65535.</p>
<p>to destination</p> <p>Edit the destination field of an existing policy.</p> <p>destination is one or more of these options:</p> <ul style="list-style-type: none"> - <i>alias if-alias</i> — if-alias is the interface alias. It must be one of these options: <i>Trusted, Optional, External, Any-Trusted, Any-Optional, or Any-External.</i> - <i>custom-address if-alias address address-format group-user type name authsvr</i> <p>* address-format must be one of these options:</p> <ul style="list-style-type: none"> • <i>host-ip</i> A.B.C.D. • <i>host-range</i> A.B.C.D W.X.Y.Z. • <i>network-ip</i> A.B.C.D/M. <p>* type is either <i>user</i> or <i>group</i>.</p> <p>* name is the user name or group name.</p> <p>* authsvr is one of these options: <i>Firebox-DB, RADIUS, LDAP, SecurID, or Active-Directory.</i></p> <ul style="list-style-type: none"> - <i>tunnel-address bovpn</i> — bovpn is the BOVPN name. - <i>user-group type name authsvr</i>
<p>traffic-mgmt tmname</p> <p>Assign traffic management to a policy.</p> <p>tmname is a traffic management configuration that was already defined.</p>

Example:

```
rule HTTP-proxy-Out
policy-type HTTP-proxy from alias Any-Trusted to alias Any-External enable
logging
schedule releaseweek
snmp
policy-routing backup External-1 failover External-2
```

schedule

Description: Build a schedule for use in policies.

Syntax:

schedule <i>name</i> time-block <i>entry</i>
<p><i>name</i> is the name of the schedule.</p> <p><i>entry</i> must be entered with this syntax: <i>period starthour startmin endhour endmin</i>.</p> <ul style="list-style-type: none"> - <i>period</i> must be one of these options: <i>daily, mon, tue, wed, thu, fri, sat, or sun</i>. - <i>starthour</i> is the hour the period starts, and must be in the range of 0 to 23. - <i>startmin</i> is the minute the period starts, and must be in the range of 0 to 60. - <i>endhour</i> is the hour the period ends, and must be in the range of 0 to 23. - <i>endmin</i> is the minute the period ends, and must be in the range of 0 to 60. <p>You can add more <i>entry</i> entries at the end of this command.</p>

Example:

```
schedule releaseweek time-block mon 5 30 19 30 tue 5 30 19 30
```

sslvpn

Description: Configure the device to enable Mobile VPN with SSL connections.

Syntax:

sslvpn enable
<p>Enable Mobile VPN with SSL on the device.</p> <p>No options available.</p> <p>Use no sslvpn enable to disable SSL VPN connections.</p>
sslvpn external address
<p>Configure Mobile VPN with SSL to use an external address or domain.</p> <p><i>external</i> is either <i>primary</i> or <i>backup</i>.</p> <p><i>address</i> is either the IP address of an external interface in the format A.B.C.D., or an alias for an external interface.</p> <p>Use no sslvpn server address to disable a backup external interface for SSL VPN.</p>
sslvpn type servers address
<p>Configure Mobile VPN with SSL to use specific DNS or WINS servers.</p> <p><i>type</i> is either <i>dns</i> or <i>wins</i>.</p> <p><i>address</i> is an IP address in the format A.B.C.D. You can add up to two servers.</p> <p>Use no sslvpn type servers address to remove a DNS or WINS server from the configuration.</p>
sslvpn dns domain-name domain
<p>Define the domain name for SSL VPN.</p> <p><i>domain</i> is a qualified domain name.</p> <p>Use no sslvpn dns domain-name domain to remove the domain name from the configuration.</p>
sslvpn resource method
<p>Define what resources are available to Mobile VPN with SSL users.</p> <p><i>method</i> must be one of these options:</p> <ul style="list-style-type: none"> - <i>user-route net</i>, where <i>net</i> is a subnet address in the format A.B.C.D./#. - <i>appliance-route</i> — enables access to a directly connected network. - <i>force-traffic</i> — forces all traffic through the tunnel. <p>Use no sslvpn resource user-route net to remove a specified network from the configuration.</p>
sslvpn address-pool net
<p>Define a subnet to be used as a virtual address pool.</p> <p><i>net</i> is a subnet address in the format A.B.C.D./#, where # is an integer from 0 to 32.</p>

sslvpn algorithm <i>type method</i>
Select the authentication and encryption methods to use to secure SSL VPN connections. <i>type</i> must be either <i>authentication</i> or <i>encryption</i> . If <i>type</i> is <i>authentication</i> , <i>method</i> must be one of these options: <i>MD5</i> , <i>SHA-old</i> , <i>SHA-1</i> , <i>SHA256</i> , or <i>SHA512</i> . The default method is MD5. If <i>type</i> is <i>encryption</i> , <i>method</i> must be one of these options: <i>Blowfish</i> , <i>DES</i> , <i>3DES</i> , <i>AES-128</i> , <i>AES-192</i> , or <i>AES-256</i> . The default method is Blowfish.
sslvpn auth-server <i>authentication</i>
Select a method to use to authenticate Mobile VPN with SSL users. The authentication method selected must already be configured for the device. <i>authentication</i> must be one of these options: <i>Firebox-DB</i> , <i>RADIUS</i> , <i>SecurID</i> , <i>LDAP</i> , or <i>Active-Directory</i> . If <i>authentication</i> is either <i>RADIUS</i> or <i>SecurID</i> you can use the optional command <i>force</i> to force users to authenticate again after a connection is lost.
sslvpn keepalive <i>setting value</i>
Configure SSL VPN keep-alive settings. <i>setting</i> must be either <i>interval</i> or <i>timeout</i> . <i>value</i> is measured in seconds and must be an integer. <ul style="list-style-type: none"> - The default value for the keep-alive interval is 10. - The default value for the keep-alive timeout is 60.
sslvpn protocol <i>protocol port</i>
Change the protocol and port used for Mobile VPN with SSL. <i>protocol</i> must be either <i>TCP</i> or <i>UDP</i> . The default is TCP. <i>port</i> must be an integer from 0 to 65535. The default is 443.
sslvpn config-port <i>config-port</i>
Change the TCP port used to negotiate the SSL VPN data channel and to download Mobile VPN for SSL configuration files. You can change the config-port only if the <i>sslvpn protocol</i> is set to UDP. If the <i>sslvpn protocol</i> is set to TCP, the config-port uses the same port you specified with the <i>sslvpn protocol</i> command. <i>config-port</i> must be an integer from 0 to 65535.
sslvpn renegotiate <i>interval</i>
Set the number of minutes a connection can be active before the device forces a renegotiation of the tunnel. <i>interval</i> must be an integer greater than 60. The default value is 60.

Example:

```
sslvpn primary 100.100.100.10
sslvpn backup 50.50.50.20
sslvpn dns servers 10.1.2.4 10.1.2.5
sslvpn dns domain-name watchguard
sslvpn address-pool 192.168.113.0/24
sslvpn authentication SHA-1
sslvpn auth-server Firebox-DB
sslvpn keepalive timeout 30
sslvpn renegotiate 90
```

traffic-management

Description: Configure a traffic management action to use with policies.

Syntax:

traffic-management *name configuration*

name is a string that uniquely identifies the traffic action.

configuration is in the format ***interface minimum maximum***.

- ***interface*** is an integer from 0 to 7.
- ***minimum*** is measured in Kbps and must be an integer from 0 to 1000000.
- ***maximum*** is measured in Kbps and must be an integer from 0 to 1000000.

You can add one or more ***configuration*** actions. The maximum number is the number of interfaces on the device.

user-group

Description: Define a user group for Firebox authentication.

Syntax:

user-group *name description desc membership user*

name is the name of the user group.

desc is a short description of the purpose of the group.

user is a user name already configured on the device.

You can add more than one user.

Example:

```
user-group accounting description Finance_and_Accounting_Dept membership
jackn gloriap cindyk karentc
```

users

Description: Define a user for Firebox authentication.

Syntax:

users *name passphrase session-timeout idle-timeout group groupname description desc*

name is a string that uniquely identifies the user.

passphrase is the unencrypted client password.

session-timeout is the duration in hours before a session times out. It must be an integer. The default value is 8.

idle-timeout is the duration in minutes before an idle session times out. It must be an integer. The default value is 30.

groupname is a Firebox authentication user group.

desc is a brief description of the user.

Example:

```
users jackp somethingeasy 24 60 group executives description Jack_Parase_CEO
```

Index

Symbols

? 5, 8, 16, 17

A

Active Directory
 configure server 75
 groups used as alias 73
address pool
 used for DHCP 52, 65
 used for PPTP 88
 used for SSL VPN 93
admin
 connecting to the device as 4
 prompt 13
administrator accounts 4
alarm
 configure for rule 90
 send to remote log server 47
 traffic from blocked site 45, 46
 traffic to blocked port 45
alias
 assign to interface 68
 create and modify 73
 show interface aliases 19
 use for authentication 74
allowed site
 add or remove address 45
 import from file 32
 show IP settings for 18
ambiguous command 9
antivirus 54
apply 74
ARP
 arp flush 25
 flush table 25
 show table 17
authentication 95
 auth-server 75
 auth-setting 39
 auth-user-group 76
 configure aliases for 74
 configure server 75

 configure service 39
 configure user groups 76
 Firebox users *See* users
 show authorized users and groups 19
 show global settings 19
 show server 19
 used for SSL VPN 94
 user groups *See* user groups
 web-server-cert 57

B

backup image 25
blocked port
 log messages 45
 show IP settings for 18
 specify port(s) 45
blocked site
 add IP address 45
 add site 47
 configure 45
 flush status 46
 import from file 32
 set duration 45
 show settings 18
BOVPN
 gateway
 bovpn-gateway 77
 force rekey 35
 show settings 19
 tunnel
 bovpn-tunnel 79
 create alias 73
 create or modify 79
 show active 18
 show settings
bovpn-tunnel *See* BOVPN
branch office *See* BOVPN
bridge
 assign name 40
 enable mode
bulk license 32

C

- certificates
 - cert-request 25
 - import from file 32
 - import from Management Server 48
 - issue certificate 25
 - show available 20
 - use device to issue 25
 - web server 57
 - web-server-cert 57
- change passwords 32
- checksum 26
- CLI
 - debugging 26
 - entering commands 5
 - exiting 16
 - getting help 5
 - prompt 13
 - starting 3
- clock
 - change time 26
 - clock 17, 26
 - show settings 17
- cluster
 - display diagnostic information 27
- command mode 11
 - Configuration 12
 - Interface 12
 - Main 12
 - Policy 12
- common commands
 - introduction 13, 15
 - list of commands 15
 - reference 16
- configuration
 - import from file 32
 - restore from prior 33
 - update 74
- Configuration command mode
 - accessing 38
 - introduction 12, 37
 - list of commands 38
 - reference 39
- configure settings 49
- configure users 95
- connect 3
- console port 3
- contact 55

D

- dangerous activity 39, 40, 43
- DDNS *See* dynamic DNS
- DDoS 43
- debugging
 - CLI 26
 - configure type and level 47
 - debug-cli 26
 - send messages to remote server 47
- default packet handling
 - configure 42

- configure logging 39, 42
- dangerous activity 39, 40, 43
- DDoS 43
- default-packet-handling 17
 - show settings 17
 - unhandled 39, 40, 42
- default password 4
- device name 55
- DHCP
 - dchp 65
 - enable as relay 52, 65
 - enable as server 52, 65
- diagnose 28
- diagnostic information 28
- Diffie-Helman 77
- DNS
 - add or remove server 39, 40, 41, 46
 - dnslookup 31
 - set domain name 46
 - used for authentication server 75
 - used for DHCP server 52, 65
 - used for SSL VPN 93
- DNS lookup 24
- domain name
 - used for BOVPN 77
 - used for certificate request 25
 - used for dynamicDNS 42
 - used for SSL VPN 93
- drop-in mode
- duplex 66
- dynamic DNS
 - configure device for 42
 - show settings 20
- dynamic NAT
 - configure 81
 - enable in rule 90
 - show 17
- dynamic routing
 - set protocol 46
 - show settings 17

E

- engine 54
- enter commands 5
- error messages 8
- e-Series 1
- event messages
 - enable logging 47
 - send to remote server 47
- execution error 8
- exit 16
- export
 - export 3, 31
 - files from device 9
- External interface 70

F

- factory default

- restore to 33
- show 17
- FastEthernet 44
- feature keys
 - features 17
 - import from file 32
 - show 19
 - show active features 17
 - synchronize between devices
- fingerprint 20
- Firebox authentication 76
- FireCluster members 18
- firewall action 90
- flash disk *See* backup image
- friendly name 55
- FTP files 9

G

- gateway *See* BOVPN
- GAV signatures 17
- global settings
 - device properties 55
 - disable for specified rule 89
 - enable VPN 56
 - override QoS by rule 91
 - show authentication 19
 - show for device 19
 - show VPN 18
- groups *See* user groups

H

- help 5, 16
 - ? 8
 - syntax 6
- history 2, 17

I

- ICMP
 - icmp 90
 - set traffic action 90
- idle timeout
 - set for rule 90
- interface command mode
 - interface 44
- IKE gateway 79
- IKE packet trace
 - show log settings 18
- import
 - bulk license 32
 - files to device 9
 - import 32
 - route configuration 32
- incomplete command 8
- interface
 - configure address 66
 - configure options 66

- configure speed and duplex 66
- create alias 73
- MAC address binding 67
- multi-WAN probe 51, 52
- name 68
- set multi-WAN sequence 51
- Interface command mode
 - accessing 43, 44, 64
 - interface 43
 - introduction 12, 63, 71
 - list of commands 64
 - reference 65
- Internet Protocol settings 18, 45
- intrusion prevention 17, 42
- ip 45, 66
- IPS signatures 17, 54
- IPSec pass through 56

K

- keep alive
 - for SSL VPN 94

L

- LDAP
 - configure server 75
- licenses *See* feature keys
- link-speed 66
- load balancing
 - by policy 92
 - set sequence for multi-WAN 51
- local gateway 77
- location 55
- log messages
 - blocked ports 45
 - default packet handling 39, 42
 - enable by category 47
 - send to remote server 47
- log server
 - configure 47
 - show settings 18
- log settings
 - diagnostic logging 18
 - IKE packet trace 18
 - internal storage 18
 - log firebox traffic 18
 - log server 18
 - log-cache 18
 - log-settings 47, 58
 - performance statistics 18
 - show settings 18
 - traffic messages 18
- logged in users 17, 35
- logging *See* log settings

M

- MAC access control
 - configure 67

- mac-access-control 67
- MAC address binding
 - configure 67
 - mac-ip-binding 67
 - show settings 17
- Main command mode
 - accessing 24
 - introduction 12, 23
 - list of commands 24
 - reference 25
- managed client
 - configure secondary server 48
 - enable device 48
 - import certificate 48
 - managed-client 17
 - set primary server 48
 - show settings 17
- Management Server 48
- Mobile VPN with PPTP
 - show active users 18
- mode *See network mode.*
- modem
 - modem failover 49
- mtu 67
- multi-WAN
 - load balance failover 51
 - method to check status 51, 52
 - show settings 17
- MVPN
 - configure with IPsec 82, 85
 - mpn-ipsec 82, 85
 - show IPsec group configuration 19

N

- name *See interface* 68
- NAT
 - one to one 87
 - static NAT 92
- network
 - create alias 73
- network mode
 - mode
 - network-mode 17
 - show settings 17
- notation 2
- NTP
 - configure 53
 - show settings 17

O

- one-to-one-nat
 - one-to-one-nat 87
 - show settings 17
- operating system 34, 35
- Optional interface 3, 70
- outbound access list
 - remove all IP addresses 39
 - remove an IP address 39
 - show allowed IP addresses 17

P

- password 32
- performance statistics
 - enable collection of 47
 - show settings 18
- ping 32
- policy 53
- Policy command mode
 - accessing 53, 72
 - introduction 12
 - list of commands 72
 - policy 53
 - reference 73
- policy *See rule* 89
- policy template
 - create custom 87, 88
 - policy-type 87, 88
 - show settings 19
- policy-type *See policy template*
- PPTP
 - configure address pool 88
 - configure firewall to allow 88
 - pptp 88
 - show settings 17
- prompt 13
 - WG(Config)# 13
 - WG(config/if-fe0)# 13
 - WG(config/policy)# 13
 - WG# 4, 13, 24
 - WG> 4, 24

Q

- QoS
 - configure 69
 - override for rule 91
 - override marking by rule 91
- quit 16

R

- RADIUS
 - configure primary server 75
 - use for tunnel authentication 73
- read only 4, 13, 24
- read write 4, 13, 24
- read-only password 32
- read-write password 32
- reboot 32
- reference
 - common commands 16
 - Configuration command mode 39
 - Interface command mode 65
 - Main command mode 25
 - Policy command mode 73
- rekey BOVPN gateway 35
- remote gateway 77
- restart *See reboot*
- restore 33

- round robin 51
- route
 - create static 46
 - import from file 32
 - show settings 17
 - traceroute 34
- routed mode
- rule
 - configure 89
 - configure alarm 90
 - configure firewall action 90
 - enable 89
 - enable dynamic NAT 90
 - enable features 91
 - enable logging 91
 - enable QoS 91
 - enable SNMP 92
 - override QoS by rule 91
 - set idle timeout 90
 - show specification 19
 - use policy-based load balancing 92
 - use static NAT 92

S

- saving changes 74
- schedule
 - configure 93
 - show settings 19
- SecurID
 - configure primary server 75
- serial cable 3
- server load balancing *See* load balancing
- set network mode
- show
 - active BOVPN tunnels 18
 - active Mobile VPN with PPTP users 18
 - alias 19
 - arp 17
 - authentication server 19
 - authorized users and groups 19
 - auth-setting 17, 19
 - bovpn-gateway 19
 - branch office VPN IPSec proposal settings 19
 - certificate 20
 - certificate fingerprint 20
 - clock 17
 - component 17
 - ddns
 - default-packet-handling 17
 - dynamic-nat 17
 - factory-default 17
 - feature-key 19
 - features 17
 - FireCluster settings 18
 - global-settings 19
 - ip 18
 - login-user 17
 - log-settings 18
 - managed-client 17
 - max allowed outbound IP addresses 17
 - multi-wan 17
 - mvpn-ipsec 19
 - network-mode 17

- ntp 17
- one-to-one-nat 17
- policy-type 19
- pptp 17
- route 17
- rule 19
- schedule 19
- signature-update 17
- snmp 17
- sslpvpn 17
- static-arp 17
- status-report 17
- sysinfo 18
- traffic-management 19
- upgrade 18
- user-group
- users
- shutdown 33
- signature update
 - configure 54
 - show last date 17
 - signature update 54
 - signature-update 17
- single sign on
 - show settings 19
- SNMP
 - configure device for 54
 - enable trap for rule 90
 - show settings 17
 - snmp 17, 54
- speed 66
- SSL VPN
 - configure 93
 - show settings 17
- start CLI 3
- static NAT 92
- static-arp 55
 - show 17
- status
 - connecting to the device as 4
 - prompt 13
- status report 17
- support messages
 - send to remote server 47
- sync
- syntax
 - error 9
 - help command 6
 - reference notation 2
- system
 - display network mode 17
 - set network mode
 - system 55
- system information
 - configure properties 55
 - show settings 18, 34
 - sysinfo 18, 34

T

- TCP
 - tcpdump 34
- TCP/IP 3

- terminal client 5
- terminal commands 5
- TFTP files 9
- time *See* clock
- timestamp 53
- timezone
 - configure 55
- traceroute 34
- traffic management
 - configure action 95
 - show action 19
- traffic messages
 - send to remote server 47
 - show log settings 18
- transform 77
- Trusted interface 3, 70
- type 70
- Type of Service 56

U

- unhandled packets 39, 40, 42
- unrecognized command 8
- update
 - configuration 74
 - IPS/AV engine 54
 - signatures 17, 54
- upgrade
 - from image 34, 35
 - show audit trail 18
 - upgrade 34, 35
- user groups
 - configure for authentication 76
 - create alias 73
 - show settings 19
 - user-group 95
- users
 - define for Firebox authentication 95
 - logged in 17
 - show users 19

V

- VLAN *See* bridge
- VPN
 - configure PMTU settings 70
 - enable global settings 56
 - show global settings 18
 - vpn-setting 18, 56
 - vpn-tunnel 35

W

- WG(config)# 13, 38
- WG(config/if-fe0)# 13, 44, 64
- WG(config/policy)# 13, 53, 72
- WG# 4, 13, 24
- WG> 4, 13, 24
- who 35

- WINS
 - configure servers 46
 - show IP settings for 18
 - used for authentication 75
 - used for DHCP 52, 65
 - used for SSL VPN 93

X

- XTM 1